UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERÍA

MAESTRIA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

II EDICION

"Diseño e implementación de un DRP (Disaster Recovery Plan) para Departamento de Ingenierías de la Empresa Continental Tire Andina."

TESIS PREVIO A LA OBTENCIÓN DEL TITULO DE MAGISTER EN GERENCIA DE SISTEMAS DE INFORMACIÓN

AUTOR: Ing. Marcelo Rolando Ávila Vásquez

DIRECTOR: Ing. Juan Alberto Herrera Silva MSc.

CUENCA-ECUADOR

2013

RESUMEN

El presente trabajo constituye un documento de apoyo dentro de la empresa Continental Tire Andina S.A. para su plan de recuperación ante desastres. En este documento constan el análisis y diseño de planes, procedimientos para salvaguardar el bien más preciado de la empresa que es la información dentro de su sistema integrado de manufactura SIM y sus aplicaciones en el departamento de Ingenierías.

En el primer capítulo se presenta el análisis previo para el desarrollo de este trabajo como son los objetivos planteados y la justificación para una implementación dentro la empresa alineados con sus objetivos estratégicos.

El segundo capítulo se refiere al sustento teórico utilizado para elaborar este documento, como son las definiciones y terminología, normas, políticas, metodologías, etc.

En el capítulo tres se realiza un análisis de la situación actual de la empresa, y se realiza un mapeo de las principales amenazas y vulnerabilidades, lo cual nos sirve para medir el nivel de impacto que tienen ciertos procesos y sistemas de información dentro de la empresa. Para los capítulos cuatro y cinco de la tesis ya consta la elaboración de los planes BIA y de procedimiento DRP que se va adoptar para una solución a medida dentro de la empresa bajo las mejores prácticas. Finalmente, el capítulo seis hace referencia a las conclusiones y recomendaciones

PALABRAS CLAVES:

DRP, SIM, SCADA, PLC, IPC, OPC, BACKUP.

ABSTRACT

This work is a document of support within the company Continental Tire Andina SA plan for disaster recovery. In this paper the analysis and design consist of plans, procedures to safeguard the most valuable company information is well within your SIM integrated manufacturing system and its applications in the engineering department .

The previous analysis for the development of this work as are the objectives and rationale for implementation within the company aligned with its strategic objectives is presented in the first chapter.

The second chapter deals with the theoretical basis used to prepare this document, as are the definitions and terminology, rules, policies, methodologies, etc.

In the third chapter analyzes the current situation of the company is carried out, and a mapping of the major threats and vulnerabilities is performed, which serves to measure the level of impact that certain processes and information systems within the company.

For chapters four and five of the thesis and includes the preparation of plans and DRP BIA procedure to be adopted for a customized solution within the company on best practices.

Finally, chapter six refers to the conclusions and recommendations.

KEY WORDS:

DRP, SIM, SCADA, PLC, IPC, OPC, BACKUP.

ÍNDICE DE CONTENIDOS

DECLARACION

Yo, **Marcelo Rolando Ávila Vásquez**, autor de la tesis **"Diseño e implementación de un DRP (Disaster Recovery Plan) para Departamento de Ingenierías de la Empresa Continental Tire Andina."**, reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de Magister en Gerencias de Sistemas de Información. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autor.

Cuenca, 04 diciembre de 2013

Marcelo Rolando Ávila Vásquez
C.C: 0103749594

CERTIFICACIÒN

Yo, **Marcelo Rolando Ávila Vásquez**, autor de la tesis **"Diseño e implementación de un DRP (Disaster Recovery Plan) para Departamento de Ingenierías de la Empresa Continental Tire Andina."**, certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor.

Cuenca, 04 diciembre de 2013

_____
Marcelo Rolando Ávila Vásquez
C.C: 0103749594

Quito, 04 de diciembre del 2013

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Ing. Marcelo Rolando Ávila Vásquez , bajo mi supervisión.

Atentamente,

Msc Ing. Juan Herrera S.
DIRECTOR DE TESIS

DEDICATORIA

A Dios, quien me dio la fe, la fortaleza, la salud y la esperanza para terminar este trabajo.

A mis hijos, David Sebastián y Marcelito Nicolás, que con su presencia ha iluminado nuestras vidas, y por quien vale todo el sacrificio hecho para que en el futuro se sienta orgulloso de su papá.

A mi esposa, Diana María, siempre con sus consejos y amor. ¡Tu presencia en mi vida ha sido una bendición, te amo!

A mis padres, por su esfuerzo para darme los estudios, que de alguna manera este triunfo pueda recompensar ese sacrificio.

Marcelo Rolando

AGRADECIMIENTO

En primer lugar agradezco a Dios por darme la existencia, mi familia y tres grandes amores en esta vida… mi esposa Diana María, mis hijos David Sebastián y Marcelito Nicolás.

A mis compañeros de trabajo, Carlos, Luis, Christian, Byron, Paul, Hernán, que gentilmente me colaboración en la realización y consultas para la elaboración de este tema.

A mis padres por su amor y apoyo incondicional durante todos estos años, sin su esfuerzo no habría podido haber culminado con mis estudios.

A mi esposa por su amor y aliento en los momentos difíciles.

A mis hermanos por siempre estar a mi lado y familiares políticos.

A mi director Ing. Juan Herrera por su valiosa ayuda y siempre sabio consejo en la consecución de este trabajo.

Y finalmente a los miembros del Tribunal por sus valiosos aportes a la culminación de este trabajo.

Gracias

Capítulo 1

Introducción

CAPITULO 1. INTRODUCCION

1.1 Antecedentes

El presente trabajo de investigación ha sido fundamentado en la necesidad de la empresa Continental Tire Andina S.A de preservar el activo más preciado, como es la información proveniente de las diferentes aplicaciones electrónicas e informáticas (área de TI) para el proceso de fabricación de neumáticos.

Al no disponer de normas, políticas, procedimientos y metodologías ágiles al momento de restaurar el servicio en las aplicaciones y equipos se producen cuantiosas pérdidas económicas y de la preciada información histórica para reportes (proceso, calidad, incidentes, etc.).

En la actualidad toda empresa necesita ser eficiente y estar regulada por las mejores prácticas y modelos para mejorar su productividad y calidad, al poseer tecnología innovadora y competitiva como SIM (System Integrated Manufactury), por lo que es parte fundamental garantizar la continuidad servicio alineado con el Plan Continuidad del Negocio.

La empresa al contar con el sistema integrado de manufactura conjuntamente con el ERP implementado (en este caso: SAP-estándar de Continental AEG), demanda un alto aseguramiento de la continuidad del servicio en la planta por tanto se debe implementar planes y procedimiento efectivos y eficaces para restaurar el servicio en caso de presentarse cualquier tipo de eventualidades.

Teniendo como antecedente lo expuesto en los párrafos anteriores el objetivo principal consistirá en hacer un estudio en la empresa y establecer los planes, procedimientos, metodología base para mitigar riesgos y salvaguardar la información del sistema SIM.

1.2 Problemática

El avance tecnológico en los últimos años es impresionante, ya sea en el campo del hardware y software, se dispone de diversas herramientas y utilitarios que nos ayudan a una mejor administración y control de los datos que es considerado hoy en día el activo más preciado.

Es por eso que dentro del tema de la seguridad, confidencialidad y protección de la información, es de gran relevancia en la actualidad en las diferentes empresas e instituciones, ya que la información no debe estar expuesta a ningún peligro o amenaza en caso de presentarse una contingencia.

En la empresa Continental Tire Andina S.A. existen políticas y normas en cuanto al acceso del recurso tecnológico que se dispone, pero existe la necesidad de contar con métodos y planes efectivos que sean fácilmente aplicables y del conocimiento del personal ante la presencia de una contingencia o eventualidad mayor.

La principal debilidad que se presenta al momento de brindar el soporte necesario para superar el percance, es la falta de conocimiento personal (prioridad, tiempo, criticidad) y uso de un método ágil que nos lleve a superar rápidamente los problemas, además de la falta de recursos y herramientas informáticas.

Se cuenta con un Sistema Integrado de Manufactura (SIM), el cual es el encargado de la planificación y control total de la producción en la línea de

neumáticos, el cual recibe automáticamente la información de las diversas maquinas controladas por un Controlador Lógico Programable (PLC), convirtiéndose esta la principal fuente de vulnerabilidad y de manejo de información sensible para el área de manufactura. Se tiene un alto nivel de dependencia y la presencia de un fallo, inconveniente o problema mayor provocará grandes problemas dentro del negocio, originando perdida de información para reporte y planificación de la producción.

1.3 Justificación

Es importante que una empresa como Continental Tire Andina S.A, que posee un alto nivel de automatización tanto de sus procesos de producción de neumáticos como de sus procesos informáticos para el manejo de la información cuente con un adecuado Plan de Recuperación ante Desastres (DRP) que le permita mantener a buen recaudo sus activos y salvaguardar su tecnología.

La ventaja del diseño e implementación (según análisis) del DRP en la empresa repercutirá en los siguientes aspectos:

- Reducción de costos
- Disminución de tiempos por parada
- Facilita el respaldo y control información aplicaciones
- Entrenamiento del personal

Consciente de esta necesidad y realidad para la obtención de información oportuna y confiable dentro la empresa, que el departamento de Ingenierías requiere implementar mecanismos de recuperación y respaldo para sus distintas aplicaciones electrónicas e informáticas.

Con esta práctica se solventará los cumplimientos de metas y objetivos impuestos al realizar este trabajo.

1.4 Objetivos

Dentro de la realización el presente trabajo investigativo se ha planteado los siguientes objetivos:

1.4.1 Objetivo General

Elaborar un directorio de procedimientos, planes de contingencia en caso de presentarse eventualidades, desastres, en el sistema integrado de manufactura (SIM), dentro del departamento de Ingenierías de la Empresa Continental Tire Andina, basado en estándares y normas fijadas por la división de TI de Continental Tire Américas.

1.4.2 Objetivos Específicos

- Analizar los sistemas existentes dentro del departamento de Ingenierías para definir requisitos previos, como el tipo de información, aplicaciones (por ejemplo: el Sistema Integrado de Manufactura, los Sistemas de Control, Supervisión y Adquisición de Datos, etc.), infraestructura, entre otras.

- Especificar técnicamente los requisitos en base a los estándares y normas fijadas por Continental Tire Américas, necesarios para establecer, implantar e implementar un DRP dentro del departamento de Ingeniería de la empresa Continental Tire Andina S.A.

- Definir una Metodología basada en el o los estándares fijadas por Continental Tire Américas, que permita elaborar el plan de contingencia y salvaguardar la información de las diferentes Aplicaciones administradas por el Departamento de Ingeniería de la Empresa Continental Tire Andina S.A.

- Determinar los recursos necesarios y el impacto así como de los beneficios que provocará la implementación del DRP en la empresa Continental Tire Andina S.A

Capítulo 2

Marco Teórico

CAPITULO 2. MARCO TEORICO

2.1 Definición de conceptos

Para la realización del presente trabajo es necesario definir algunos conceptos básicos acerca de los equipos, aplicaciones y servicios que se disponen en la empresa, además de los estándares y metodologías a utilizar para desarrollar el mismo.

2.1.1. Definición de DRP

El termino DRP proviene de sus siglas en ingles Disaster Recovery Plan, el cual hace referencia al Plan que deben disponer las empresas u organización para en caso de existir o presentarse un desastre natural o causado por humanos que permita restablecer sus operaciones de negocio en un tiempo preestablecido, en el caso de la empresa Continental Tire Andina enfocado a Sistema Integrado de Manufactura y sus aplicaciones del Departamento de Ingenierías.

Un DRP debe estar enfocado, tanto en Software como en Hardware crítico para el proceso de negocio, además de un análisis de riesgo que identifique los *diferentes riesgos*[1] susceptibles a una empresa y que pueden impactar negativamente las operaciones normales de una organización. Generalmente el DRP es flexible a las necesidades de cada empresa y puede ser modular adaptándose a los requisitos en la organización.

Para un DRP entre más tiempo permanezca sin servicios de TI, más costosas serán las consecuencias para la empresa, pero por otra parte el costo de los sistemas de recuperación aumentan de acuerdo a que tan rápido puedan recuperar sus Sistemas de TI por lo que el objetivo de este presente trabajo será

[1] Diferentes riesgos, por ejemplo: inundaciones, incendios, falla de suministro de energía, huelgas, etc.

encontrar un equilibrio para que la empresa encuentre la inversión adecuada para su Sistemas de Recuperación de Desastres.

En conclusión el principal objetivo de un Plan de Recuperación de Desastres es dar a la organización la capacidad de recuperar las operaciones del negocio después de presentado un desastre o interrupción. Con el fin de recuperar la operación normal del negocio.

2.1.2. Definición del SIM

El alto grado de avance de la tecnología computacional y de informática en los últimos años ha permitido la creación de nuevos conceptos y metodologías para la realización de los procesos de manufactura, esto ha generado la aparición del término SIM que significa Sistema Integrado Manufactura, que hace referencia a la utilización de las herramientas informáticas (software) para el control, programación, monitoreo, visualización en tiempo real de las diferentes etapas de un proceso de fabricación de un determinado producto.

La característica tecnológica de esta nueva revolución industrial es la posibilidad de la completa automatización de los equipos y maquinaria en las industrias, así como la integración de sus operaciones. Por lo que, se pueden mejorar sustancialmente la productividad y la eficiencia de sus procesos, lo que afecta positivamente la calidad de los productos y sus costos de fabricación.

Actualmente la tendencia de las empresas, es contar con un Sistema Integrado de Manufactura en las que les permita una mejor administración de sus líneas tradicionales de ensamble, brindándoles una mejor planeación de la producción, manejo de inventarios, materias primas, flexibilidad para producir diferentes productos, manejo de demandas, incrementando la productividad de la empresa.

Debido a la importante presencia que han adquirido los Sistemas de Manufactura Integrados por Computadora en la Industria actual, que actualmente se ha incrementado la demanda de personal calificado para el desarrollo, control y mantenimiento de este tipo de sistemas.

2.1.3. Definición de SCADA

Proviene de las siglas "Supervisory Control And Data Acquisition" (Control de Supervisión y Adquisición de Datos). Los sistemas SCADA son aplicaciones de software especializado, diseñadas con la finalidad de controlar y supervisar procesos a distancia. Se basan en la adquisición de datos de los procesos remotos.

Se trata de una aplicación de software, especialmente diseñada para funcionar sobre ordenadores en el control de producción, proporcionando comunicación con los dispositivos de campo (controladores autónomos, autómatas programables, etc.) y controlando el proceso de forma automática desde una computadora. Además, envía la información generada en el proceso productivo a diversos usuarios, tanto del mismo nivel como hacia otros supervisores dentro de la empresa, es decir, que permite la participación de otras áreas como por ejemplo: control de calidad, supervisión, mantenimiento, etc.

Los sistemas SCADA proveen de toda la información que se genera en el proceso productivo a diversos usuarios, tanto del mismo nivel como de otros usuarios supervisores dentro de la empresa (supervisión, control calidad, control de producción, almacenamiento de datos, etc.).

Cada uno de los ítems de SCADA (Supervisión, Control y Adquisición de datos) involucran muchos subsistemas, por ejemplo, la adquisición de los datos puede estar a cargo de un PLC (Controlador Lógico Programable) el cual toma las

señales y las envía a las estaciones remotas usando un protocolo determinado, otra forma podría ser que una computadora realice la adquisición vía un hardware especializado y luego esa información la transmita hacia un equipo de radio vía su puerto serial, y así existen muchas otras alternativas.

Las tareas de Supervisión y Control generalmente están más relacionadas con el software SCADA, en él, el operador puede visualizar en la pantalla del computador de cada una de las estaciones remotas que conforman el sistema, los estados de ésta, las situaciones de alarma y tomar acciones físicas sobre algún equipo lejano, la comunicación se realiza mediante buses especiales o redes LAN (Local Area Network). Todo esto se ejecuta normalmente en tiempo real, y están diseñados para dar al operador de planta la posibilidad de supervisar y controlar dichos procesos.

Estos sistemas actúan sobre los dispositivos instalados en la planta, como son los controladores, autómatas, sensores, actuadores, registradores, etc. Además permiten controlar el proceso desde una estación remota, para ello el software brinda una interfaz gráfica que muestra el comportamiento del proceso en tiempo real.

Generalmente se vincula el software al uso de una computadora o de un PLC, la acción de control es realizada por los controladores de campo, pero la comunicación del sistema con el operador es necesariamente vía computadora. Sin embargo el operador puede gobernar el proceso en un momento dado si es necesario.

Un software SCADA debe ser capaz de ofrecer al sistema:

- Posibilidad de crear paneles de alarma, que exigen la presencia del operador para reconocer una parada o situación de alarma, con registro de incidencias.

- Generación de datos históricos de las señales de planta, que pueden ser volcados para su proceso sobre una hoja de cálculo.

- Ejecución de programas, que modifican la ley de control, o incluso anular o modificar las tareas asociadas al autómata, bajo ciertas condiciones.

- Posibilidad de programación numérica, que permite realizar cálculos aritméticos de elevada resolución sobre la CPU del ordenador.

Existen diversos tipos de sistemas SCADA dependiendo del fabricante y sobre todo de la finalidad con que se va a hacer uso del sistema, por ello antes de decidir cuál es el más adecuado hay que tener presente si cumple o no ciertos requisitos básicos:

Todo sistema debe tener arquitectura abierta, es decir, debe permitir su crecimiento y expansión, así como deben poder adecuarse a las necesidades futuras del proceso y de la planta.

- La programación e instalación no debe presentar mayor dificultad, debe contar con interfaces gráficas que muestren un esquema básico y real del proceso

- Deben permitir la adquisición de datos de todo equipo, así como la comunicación a nivel interno y externo (redes locales y de gestión)

- Deben ser programas sencillos de instalar, sin excesivas exigencias de hardware, y fáciles de utilizar, con interfaces amigables para el usuario.

2.1.4. Definición de PLC

El término PLC proviene de las siglas en inglés: Programmable Logic Controler, que traducido al español se entiende como “Controlador Lógico Programable”. Se trata de un equipo electrónico (Ver figura 1), que, tal como su mismo nombre lo indica, se ha diseñado para programar y controlar procesos secuenciales en tiempo real. Por lo general, es posible encontrar este tipo de equipos en ambientes industriales.

Figura1. Controlador Lógico Programable- PLC

Para que un PLC logre cumplir con su función de controlar, es necesario programarlo con cierta información acerca de los procesos que se quiere secuenciar. Esta información es recibida por captadores, que gracias al programa lógico interno, logran implementarla a través de los actuadores de la instalación.

Los controladores lógicos programables (PLC´s) tienen un sistema basado en un *microprocesador*[2] que es usado para controlar procesos y máquinas en una infinidad de líneas industriales.

El primer controlador fue diseñado por la corporación Gould en 1968 para la General Motors, para reemplazar las líneas de eléctricas de los relevadores usados en el control automático de sus líneas de transferencia. La razón por la que se implemento esta tecnología fue para hacer más fácil los cambios de secuencias de las operaciones de las máquinas en su reprogramación. Hoy en día

los controladores programables están teniendo un rápido crecimiento dentro de la industria, y esta tecnología lleva a incrementar en millones de dólares las ganancias de la industria.

Dentro de las funciones que un PLC puede cumplir se encuentran operaciones como las de detección y de mando, en las que se elaboran y envían datos de acción a los preaccionadores y accionadores. Además cumplen la importante función de programación, pudiendo introducir, crear y modificar las aplicaciones del programa.

Dentro de las ventajas que estos equipos poseen se encuentra que, gracias a ellos, es posible ahorrar tiempo en la elaboración de proyectos, pudiendo realizar modificaciones sin costos adicionales. Por otra parte, son de tamaño reducido y mantenimiento de bajo costo, además permiten ahorrar dinero en mano de obra y la posibilidad de controlar más de una máquina con el mismo equipo. Sin embargo, y como sucede en todos los casos, los controladores lógicos programables, o PLCs, presentan ciertas desventajas como es la necesidad de contar con técnicos calificados y adiestrados específicamente para ocuparse de su buen funcionamiento.

2.1.5. Definición de OPC

"El **OPC** (*OLE for Process Control*) es un estándar de comunicación en el campo del control y supervisión de procesos industriales, basado en una tecnología Microsoft, que ofrece un interface común para comunicación que permite que componentes de software individuales interaccionen y compartan datos", es decir es un driver genérico que proporciona cada fabricante para interface de comunicación bajo sistema operativo Windows.

Permite a las aplicaciones leer y escribir valores de proceso y que los datos sean compartidos fácilmente en una red de ordenadores.

La comunicación OPC se realiza a través de una arquitectura Cliente-servidor. En donde el servidor OPC es la fuente de datos (como un dispositivo hardware a nivel de planta) y cualquier aplicación basada en OPC puede acceder a dicho servidor para leer/escribir cualquier variable que ofrezca el servidor.

Es una solución abierta y flexible al clásico problema de los drivers propietarios (cada software requería un driver distinto para cada hardware, implicando un esfuerzo enorme, al que hay que añadir el de las actualizaciones continuas). Prácticamente todos los mayores fabricantes de sistemas de control, instrumentación y de procesos han incluido OPC en sus productos.

Con OPC, los fabricantes de hardware sólo tendrán que preparar un conjunto de componentes de software para que los clientes los utilicen en sus aplicaciones. Los desarrolladores de software no tendrán que reescribir los drivers debido a nuevas versiones de hardware. Los usuarios finales tendrán muchas más alternativas de integrar distintos sistemas.

2.1.6. Definiciones y términos DRP

Amenaza. "Probabilidad de que un fenómeno, de origen natural o humano, se produzca en un determinado tiempo y espacio. Peligro potencial de que las vidas o bienes materiales humanos sufran de un perjuicio o daño".[2]

Amenaza Natural. Eventos causados por la naturaleza que tiene potencial para impactar en una organización.

[2] www.crid.or.cr, Material de capacitación conceptos básicos, http;www.crid.or.cr/crid/esp/conceptos básicos.html

Análisis de Riesgo. "El análisis de riesgo involucra identificar las amenazas más probables y analizar las vulnerabilidades relacionadas con las amenazas en la organización".[3]

Para el análisis de riesgos es necesario identificar: recursos, amenazas y las vulnerabilidades en el entorno informático del Área IT.

Para tratar de minimizar los efectos de un problema de seguridad, se realiza el análisis de riesgo, término utilizado para responder tres preguntas básicas sobre la seguridad de la organización.

- ¿Qué está bajo riesgo?
- ¿Cómo se puede producir?
- ¿Cuál es la probabilidad de que suceda?

Audit Tails. Registros de eventos sobre sistema operativo, aplicaciones o actividades del usuario.

Backup. Copia de archivos y programas que facilitan la recuperación de información en caso de ser necesario.

Business Impact Analysis (BIA). "El análisis de impacto en el negocio (BIA) ayuda a identificar y priorizar los sistemas críticos IT y sus componentes".[4]

La fase del Análisis de impacto en el Negocio (BIA), identifica el impacto potencial de eventos no controlados y no específicos en los procesos del negocio de la empresa, también debe determinar qué y cómo el riesgo está identificado y priorizado dentro de las funciones críticas del negocio. Debe estimar el máximo tiempo fuera de servicio aceptable para los procesos críticos del negocio, el punto de recuperación, los objetivos, transacciones y los costos asociados con el tiempo

[3] www.drj.com, Risk analysis techniques, http;//www.drj.com/new2dr/w3_030.htm
[4] Thomas Ray, Contigency Planning Guide for Information Technology Systems, NIST 800-34, p.6.

fuera de servicio. Los tipos de criterios que pueden usarse para evaluar el impacto incluyen: servicio al cliente, funcionamiento interno, legal/estatutos y financiero.

Business Continuity Plan (BCP). Plan de Continuidad del Negocio (BCP) se enfoca en sostener las funciones del negocio de una organización durante y después de una ruptura. Un ejemplo de una función comercial puede ser el proceso de nómina de la organización o proceso de información al consumidor. Un plan de continuidad del negocio (BCP), puede escribirse para un proceso específico del negocio o puede dirigirse a los procesos claves del negocio.

Los sistemas del Área IT se consideran en el Plan de Continuidad del Negocio (BCP), debido a su apoyo en los procesos comerciales. En algunos casos, el BCP no puede direccionarse a la recuperación a largo plazo de procesos y devolver al funcionamiento normal, solamente cubre de manera provisional, los requisitos de continuidad del negocio.

Dentro del Plan de Continuidad del Negocio, se puede añadir: el Plan de Recuperación de Desastre, Plan de Recuperación del Negocio (Business Recovery Plan – BRP) y el Plan de Emergencia para el Personal (Occupant Emergency Plan – OEP). Las responsabilidades y prioridades que se encuentran en el BCP deben coordinarse con aquellos que están en el Plan de Continuidad de Operaciones (COOP) para eliminar los posibles conflictos.

Cold Sites. Un sitio alterno que esta provisto con la infraestructura ambiental y se requiere recuperar las funciones críticas del negocio o sistema de información, pero no tiene pre-instalado el hardware, equipo de comunicaciones, líneas de comunicación, etc. Estos deben aprovisionarse en el momento del desastre.

Desastre. Desastre es un súbito, no planeado evento calamitoso que causan gran daño o pérdida. La descripción de desastre puede sugerir sólo lo referente a las calamidades mayores como bombas, terremotos, guerras, etc. Además se puede considerar como un desastre la interrupción prolongada de los recursos informáticos (información de los sistemas, redes, componentes de Hardware y Software) y de comunicaciones de una organización, que no puede remediarse dentro de un periodo determinado aceptable y que necesita el uso de un sitio o equipo alterno para su recuperación.

Disponibilidad. El sistema contiene información o proporciona servicios que deben estar disponibles puntualmente para satisfacer requisitos o evitar pérdidas importantes.

Electronic Vaulting. Es el respaldo de los datos remitidos electrónicamente a un servidor fuera de sitio o facilidad de almacenamiento. La bóveda elimina la necesidad de transportar la cinta y por consiguiente acorta significativamente el tiempo requerido para mover los datos a otro lugar.

Estrategia recuperación. Procedimientos que aseguran la continuidad del negocio ante un desastre o interrupción prolongada.

Evaluación Riesgos. Lista de riesgos ordenados por su impacto y su probabilidad de concurrencia.

Firewall. Dispositivo que se instala en la red para salvaguardar las aplicaciones de intrusos intencionales y no intencionales.

Hot Site. Sitio alterno de procesamiento de datos, totalmente operacional equipado con hardware y software del sistema para ser usado en caso de desastre.

Identificación de amenazas. El proceso de identificar situaciones o condiciones que tiene el potencial de causar lesiones a personas, daños a la propiedad, o daños al ambiente.

Interrupción. Cuando un activo se pierde o no se puede utilizar.

Integridad. La meta de seguridad que genera el requisito de protección contra el intento intencional o accidental de violar la integridad de los datos (la propiedad que los datos tiene cuando no se ha alterado de una manera desautorizada) o integridad del sistema (la calidad que un sistema tiene cuando realiza su función, libre de la manipulación desautorizada). El sistema contiene información que debe protegerse de modificaciones no autorizadas, imprevistas o accidentales.

Industrial Personal Computer (IPC). Este término se utiliza para referirse a los computadores utilizados en la industria, caracterizada por ser de altas prestaciones de procesamiento, fuente de poder robusta y gran capacidad de disipación para soportar altas temperaturas de trabajo, por ejemplo: IPC Beckhoff CP6140

Maximum Allowable Outage (MAO). Cantidad de tiempo que el proceso puede estar fuera sin causar daño a la empresa o a los clientes.

Mobile Site. Transporte autónomo que cuenta con específicos equipos y telecomunicaciones necesarias para proporcionar las capacidades de recuperación total, una vez que se ha notificado de un desastre inminente o interrupción prolongada.

Operación degradada. El sistema sigue funcionando en presencia de errores con una pérdida parcial de funcionalidad o prestaciones hasta la reparación del fallo.

Periodo de recuperación. El periodo de tiempo entre el desastre y el retorno a las funciones normales durante el cual el Plan de Recuperación de Desastre es empleado.

Procesos críticos. Son aquellos sin los que sería difícil garantizar la calidad en el cumplimiento del servicio, es decir, son procesos significativos vinculados a cada tipo de organización. Cada organización debe definir cuáles son aquellos procesos que considera críticos.

Recuperación. Proceso de planear para y/o llevar a cabo la implementación de operaciones para dirigirse en el menor tiempo posible a las operaciones del negocio seguido de una interrupción o desastre.

Recovery Time Objectives (RTO). Objetivos de Tiempo de Recuperación (RTO) es el periodo de tiempo dentro del cual deben recuperarse los sistemas, aplicaciones o funciones después de una interrupción (por ejemplo un día en el negocio). El RPO se usa a menudo como la base para el desarrollo de estrategias de recuperación y como un determinante para saber si se lleva o no a cabo las estrategias durante una situación de desastre.

y como un determinante de la cantidad de datos que pueden necesitar ser recreados

Recovery Point Objectives (RPO). Objetivos de Puntos de Recuperación (RPO), es el punto en el tiempo para que los sistemas y la mayoría de los datos se recupere después de una interrupción. El RPO se usa a menudo como la base para el desarrollo de estrategias auxiliares y como un determinante de la cantidad de datos que pueden ser recreados después que se han recuperad los sistemas o funciones.

Remote Mirroring. Copiar los datos escritos en un disco o arreglo de discos a un segundo disco o arreglos de discos a través de un enlace WAN.

Riesgo. Probabilidad de daños sociales, ambientales y económicos en un lugar dado y durante un tiempo de exposición determinada.

Sitio Alterno. Sitio que facilita el normal uso de procesamiento de datos y/o conducir las funciones críticas del negocio cuando las facilidades primarias son inaccesibles debido a un desastre.

Virus Informático. El virus informático es un programa elaborado accidental o intencionalmente, que se introduce o se transmite a través de disquetes o de la red telefónica de comunicación entre ordenadores, causando diversos tipos de daños a los sistemas computarizados.

Vulnerabilidad. Es la debilidad en el plan o aplicación del control dentro de un proceso, función, o facilidad que pueden promover o pueden contribuir a una ruptura.

2.2 Aspectos generales de TI para DRP

Al momento de realizar el presente trabajo, la principal pregunta que se debe realizar es ¿Por qué implementar un DRP?, para responder esta interrogante es bueno conocer todos los aspectos que engloba y el impacto que puede tener una empresa, razón por la cual a continuación mencionaremos las razones más importantes por las cuales en la empresa Continental Tire Andina S.A. se realizó este estudio.

2.2.1 Desarrollo tecnológico

Nos encontramos en una era tecnológica constantemente cambiante, para todos los diferentes productos ya sean en hardware o en software, y es así, todas las empresas ya sean grandes o pequeñas, dependen de un sistema, correo

electrónico, base de datos, equipos de comunicación, etc., en donde procesan y almacena la información de negocio (ingresos, egresos, cantidades producidas, etc.), razón por la cual deben estar preparados al momento de migrar o cambiar los sistemas informáticas debido a la aparición de nuevas versiones o por motivos de actualizaciones.

Además cabe destacar la evolución de las redes de comunicación (internet, telefonía, enlace datos, etc.) y la disminución en los costos lo que ha minorado la brecha digital ya que ha generado que sea accesible para todos, y es por esto que las empresas son más competitivas y dependen de una u otra forma de la tecnología para realizar sus actividades negocio.

Este es un aspecto importante a considerar dentro la empresa Continental Tire Andina ya que varios de sus procesos de producción depende directamente de sistemas de información para la obtención de la información, y siempre deben considerarse los nuevas versiones de los productos tanto en software como en hardware por motivos de mantenimiento y confiabilidad de la información.

2.2.2 Información

Este aspecto a considerar es el más importante, debido a que nosotros al definir el término información, hacemos relación no solo a un conjunto de datos previamente almacenado, por el contrario a datos que representan diariamente valores imprescindibles para poder cumplir con el plan, programa y cronograma de producción dentro de la Empresa Continental Tire Andina, al ser una empresa manufactura de neumáticos.

Al momento que se genera un problema con el Sistema Integrado de Manufactura esto provoca desfases en la línea de producción, impidiendo que se contabilice los neumáticos producidos para manejo de inventarios y planificación de nuevos

materiales, originando varios desfases en la producción y a su vez produciendo un nuevo aspecto a considerar como son los tiempos perdidos.

2.2.3 Tiempos perdidos

El tercer aspecto que consideraremos muy importante para el desarrollo del presente trabajo dentro de la Empresa Continental Tire Andina, son los tiempos perdidos que surgen por falta de un plan, proceso adecuado para la restauración del SIM, que actualmente se encuentra actualmente operando en la planta.

Todo el flujo de la información de producción de neumáticos se realiza a través de la comunicación de PLC y de los PC enlazados con SIM, razón por la cual un problema en este sistema informático puede provocar un tiempo indeterminado de parada de producción si no se aplica y considera dentro del DRP planteado.

Además el propio SIM nos ayuda a calcular los tiempos perdidos en cada máquina dentro del proceso de producción y con esto elaborar el reporte tiempos perdidos que por medio del departamento de Ingeniería Industrial en la empresa se mide la productividad de la maquinaria y se realiza la estimación de la producción en base a esa información obtenida.

2.3 Normas y Políticas

Una vez analizados los aspectos de la información que vamos a enfatizarnos dentro del estudio del DRP vamos a establecer algunas normas y políticas referentes a la Seguridad dentro de la empresa que debemos tomar en cuenta para la protección de la información.

Estos conceptos de normas fueron tomados de la revisión de las normas ISO 27000, 27001 y 27002 que nos dan los lineamientos en términos de Seguridad Informática.

¿Qué es una norma de Seguridad?, la definimos como un conjunto de reglas, recomendaciones y controles con el propósito de dar respaldo a las políticas de seguridad y a los objetivos desarrollados por éstas, a través de funciones, delegación de responsabilidades y otra técnicas, con un objetivo claro y acorde a las necesidades de seguridad establecidas para la empresa.

La norma ISO basada en estándares internacionales, hace referencia los siguientes aspectos dentro de sus sub secciones como son:

ISO 27000, vocabulario y definiciones
ISO 27001, especificación del sistema de gestión de la seguridad informática (SGSI)
ISO 27002, describe el código de buenas prácticas

Hay que destacar que el adoptar el lineamiento de estos estándares internacionales (que es certificable acorde a los esquemas nacionales de cada país) se garantiza las mejores prácticas pero no esto significa que por adoptar este esquema de la norma existan fallas en su desarrollo e implementación.

¿Qué es una política de Seguridad?, una política es un lineamiento para el manejo con el personal, es una forma de comunicación, ya que las misma constituyen un canal formal de actuación, en relación con los recursos y servicios que dispone la empresa.

El objetivo principal de una política en la empresa es prevenir, proteger y manejar los diferentes riesgos, sin importar el origen del mismo.

También se conoce como un canal de comunicación con los usuarios y los gerentes, ya que establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la empresa.

No se debe confundir con el conjunto de sanciones, limitaciones para las conductas del personal, más bien cada política es consciente y vigilante del personal para el uso del recurso informático dentro de la empresa.

2.4 Elaboración de Planes

A fin de delimitar el esfuerzo necesario para planificar las diferentes actividades que contemplan el diseño de un DRP para la empresa, es conveniente empezar por definir que debe incluir este plan:

- Un Mapeo de las diferentes servicios y aplicaciones
- Análisis de Riesgo
- Valoración de la situación actual
- Elaboración de Planes recuperación
- Elaboración de Plan de Acción
- Identificación Recursos Necesarios
- Inventario de equipos
- Acceso a la información
- Plan de control

Todas estas actividades serán identificadas en el alcance de la realización del presente trabajo dentro de la empresa Continental Tire Andina, la cual ya tiene un formato preestablecido para el levantamiento de las necesidades del negocio las cuales serán especificadas dentro del capítulo 4.

2.5 Metodologías agiles

La definición proporcionada por la RAE (Real Academia Lengua Española) describe al concepto como el "*Conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal*", es decir, la forma en que se hacen las "*cosas*" (los procedimientos) empleados en un determinado proceso.

Las metodologías ágiles se han incorporado de manera general a la gestión de los departamentos IT, permitiendo una mayor eficiencia en la toma de decisiones y una clara mejora de la productividad.

Dentro diferentes metodologías vamos a mencionar a las siguientes:

Scrum para gestionar el desarrollo de proyectos y de producto por uno o varios equipos.
Kanban para gestionar los mantenimientos de los sistemas y las incidencias.
DevOps para alinear con agilidad el desarrollo de sistemas y su explotación.

Las metodologías ágiles tienen unas reglas sencillas, pero su aplicación efectiva no es tan fácil y rápida como parece, incluso si se cuenta con la experiencia de quienes han ayudado en el pasado a otras empresas a llevarlo a cabo. Para tener éxito en la "agilización" de la empresa, es crítico planificar y gestionar correctamente el cambio al nuevo modelo.

La revisión de estas técnicas nos ha servido para desarrollar la actual metodología del Análisis de Riesgo conjuntamente con el desarrollo del Análisis de Impacto en el Negocio (BIA), para poder determinar un plan adecuado de DRP, para solventar

y mitigar el riesgo, amenazas y vulnerabilidades dentro del departamento de Ingenierías dentro de la Empresa Continental Tire Andina S.A.

Cabe mencionar que las técnicas y metodología empleadas en el presente trabajo están alineadas a las reglas del Negocio que exige la empresa dentro de su proceso productivo, por ejemplo podemos mencionar a las siguientes:

- Garantizar alta disponibilidad de la maquinaria y sus aplicaciones para planificación y el cumplimiento del ticket de producción.
- Equipos y maquinarias que permitan la optimización del proceso, es decir, reducción de tiempos.
- Adecuado control y monitoreo de las variables de proceso que inciden directamente en el control de calidad del producto.
- Producción de informes y seguimiento de indicadores KPI para proceso productivo
- Sistemas de Gestión que permita mejorar los costos de producción
- Facilidad de gestión de recursos, incluyendo inventario y personal.

Todos estos factores que hemos mencionado tienen por objetivo principal producir productos con altos índices de calidad de acuerdo a los estándares exigidos en la actualidad para producir una satisfacción en el cliente final.

Capítulo 3

Análisis Situación Actual

CAPITULO 3. ANALISIS SITUACION ACTUAL

3.1 Análisis de sistemas existentes

Para la elaboración del DRP, es necesario primero realizar el análisis de Riesgo dentro de la metodología de evaluación, para esto se contó con la colaboración del personal de Sistemas de la empresa Continental Tire Andina S.A. y personal del área de Ingenierías que están encargadas del desarrollo y mantenimiento de aplicaciones para el Sistema Integrado de Manufactura (SIM) dentro de la empresa.

3.1.1 Identificación del Riesgo

La etapa de identificación del riesgo se debe encontrar todos los posibles inconvenientes que pueden presentarse, antes que provoquen daños. Razón por la cual es necesario identificar los recursos y procesos críticos que conforman el área.

Además se deben identificar las amenazas que constituyen riesgos y afecten los recursos de la organización, también es necesario estimar que tan factible es que suceda cada una de las amenazas, tarea difícil por la cantidad de información.

3.1.1.1 Identificación de amenaza

El mejor método para identificar las amenazas es observar el fenómeno, que típicamente interrumpe el proceso normal del negocio. Las amenazas más comunes que pueden presentarse son: naturales, humanas y ambientales

Amenazas Naturales. Incluyen principalmente los cambios naturales que pueden afectar de una u otra manera el normal desempeño del entorno informático, entre estas tenemos:

- Fuego
- Inundaciones
- Erupciones volcánicas
- Desastres Aéreos
- Terremotos
- Tormentas Eléctricas, etc.

Es importante mencionar que para el análisis la empresa ha sufrido dos accidentes aéreos como eventos fortuitos como son: el desprendimiento del tren de aterrizaje de un avión comercial y una avioneta estrellada en las bodegas de la empresa el 25 marzo del 2006.

Amenazas Humanas. Son eventos causados por humanos como actos intencionales o acciones deliberadas, entre estas amenazas tenemos:

- Robo
- Sabotaje
- Hacker
- Virus
- Instalación del software malicioso (Mallware)
- Error de operación, etc.

Amenazas Ambientales. Estas son:

- Electricidad
- Aire acondicionado
- Contaminación

- Químicos, etc.

3.1.1.2 Identificación de vulnerabilidades

La meta en esta etapa es desarrollar una lista de vulnerabilidades que podrían originar una potencial amenaza dentro del Área de IT, En la Tabla 2.1 se presenta un ejemplo de vulnerabilidades.

Vulnerabilidad	Amenaza	Acción de la Amenaza
Se encuentran instalados rociadores de H2O en caso de incendio, pero no existe una cubierta que proteja los equipos	Fuego Negligencia del personal	Los rociadores de H2O empiezan a girar dentro del Área IT.

FUENTE: Risk Management Guide For Information Technology System (NIST)

Tabla 3.1 Ejemplo Vulnerabilidad

Los métodos recomendados para identificar las vulnerabilidades del sistema son: el origen de la vulnerabilidad, la ejecución de pruebas de seguridad del sistema y desarrollo de una lista de verificación de los requisitos de seguridad.

3.1.1.2.1 Origen de vulnerabilidad

El origen de las vulnerabilidades técnicas y no técnicas asociadas con los procesos del Área de IT pueden ser identificadas a través de una combinación de varias técnicas tales como: encuestas, entrevistas, visitas al sitio y herramientas de examimación automáticas.

3.1.1.2.2 Pruebas de seguridad del sistema

Las pruebas de seguridad del sistema utilizan métodos proactivos, que pueden ser usados para identificar efectivamente las vulnerabilidades de los sistemas en el Área de IT, dependiendo de la criticidad del sistema y la disponibilidad de los recursos, los métodos que se pueden utilizar son:

- Herramientas de examimación automática de vulnerabilidades
- Pruebas de seguridad y evaluación
- Pruebas de penetración

3.1.1.2.3 Lista de requerimientos de seguridad

Durante la identificación de las vulnerabilidades se puede desarrollar una lista de verificación (checklist) de seguridad de los sistemas del Área de TI. Esta lista contiene los estándares de seguridad básicos utilizados para evaluar e identificar las vulnerabilidades de los activos (Personal, hardware, software e información), procedimientos no automatizados, procesos y transferencia de información de los sistemas de Área IT.

La lista de verificación hace referencia a las siguientes áreas de seguridad:

- Administrativa
- Operacional
- Técnica

La tabla 3.2 presenta una lista de seguridades que se sugieren para identificar las vulnerabilidades del sistema en cada área de seguridad.

Área de Seguridad	Criterio de seguridad
Seguridad Administrativa	Asignar responsabilidades Soporte continuo Capacidad de respuesta a incidentes Valoración de riesgo Seguridad y entrenamiento técnico
Seguridad Operacional	Control de contaminación Asegurar la calidad suministro Acceso y disponibilidad de los back ups Etiquetar y almacenar los backups Controles de Temperatura en PC y Server
Seguridad Técnica	Comunicaciones Criptología Identificación y autentificación Detección del intruso Sistemas de auditoria

FUENTE: Risk Management Guide for Information Technology System

Tabla 3.2 Lista de seguridades para identificación de vulnerabilidades

3.1.1.3 Análisis de Control

El análisis de control, lo que busca es analizar los controles que ha sido implementados o sé planean implementar, para que la empresa minimice o elimine la probabilidad de que se presenten las amenazas en el área de IT.

Los controles de seguridad abarcan el uso de métodos técnicos y no técnicos. Los controles técnicos están incorporados dentro del hardware, software o firmware (ejemplo: mecanismo de control de acceso, identificación, autenticación, encriptación, software de detección de intrusos, etc.).

Los controles no técnicos se refieren a las políticas de seguridad, procedimientos operacionales, seguridad personal, física y ambiental, dentro de la organización.

Los métodos de control técnicos y no técnicos pueden ser clasificados como preventivos o detectivos. Como detallaremos a continuación:

a) Controles preventivos. Advierten sobre los intentos de violar las políticas de seguridad e incluyen controles tales como cumplimientos en el control de acceso, inscripción, y autenticación.
b) Controles detectivos. Advierten de violaciones de las políticas de seguridad y se incluyen controles tales como audoit tails, métodos de detección de intrusos y checksums.

La implementación de los controles durante el proceso de mitigación de riesgo es el resultado directo de la identificación o de las deficiencias en común de los controles planeados durante el proceso de valoración del riesgo. Una técnica para realizar el análisis de control se basa en las listas de verificación.

3.1.1.4 Determinación de la Probabilidad

En esta etapa se determina la probabilidad que una potencial vulnerabilidad asociada a una amenaza pueda afectar la infraestructura IT, para establecer esta probabilidad se debe considerar los siguientes factores:

- La motivación y capacidad del origen de la amenaza
- La naturaleza de la vulnerabilidad
- La existencia y efectividad de los controles permanentes.

En la Tabla 3.3 se describe el nivel de probabilidad que puede ser ALTO, MEDIO o BAJO.

Nivel de probabilidad	Definición de probabilidad
ALTO	El origen de la amenaza es alto, y los controles para prevenir las vulnerabilidades, por el momento son ineficientes o no existen.
MEDIO	El origen de la amenazas se encuentra presente, pero los controles pueden impedir que las amenazas afecten realmente a la empresa
BAJO	El origen de las amenazas pueden presentarse, pero existen controles que impiden que la amenaza afecte realmente a la empresa

FUENTE: Risk Management Guide for Information Technology System (NIST)

Tabla 3.3. Definición de probabilidades

3.1.1.5 Análisis de Impacto

La próxima etapa, es medir el nivel de riesgo que permite establecer el impacto adverso que se obtiene como resultado de la ejecución de una amenaza exitosa provocada por una vulnerabilidad. Antes de empezar con el análisis de impacto es necesario obtener la siguiente información:

- La misión del sistema (procesos ejecutados por el sistema)
- Sistemas, datos críticos y sensitivos.

La documentación puede ser obtenida de los documentos originales de la organización tales como: reportes de la misión del análisis de impacto o reportes de valores de criticidad de los activos. El Análisis de Impacto en el Negocio (BIA)

permite priorizar los niveles de impacto asociados con el compromiso de la organización.

La información de activos basados en la valoración cualitativa o cuantitativa de la sensibilidad y criticidad de los activos. Un activo se valora como crítico, mediante la identificación, priorización de la información y sensitividad de los activos de la empresa. (Por ejemplo: hardware software, sistemas, servicios y activos relacionados con la tecnología) que soportan procesos críticos dentro de la organización.

Si esta documentación no existe o la valoración para la organización de los activos del Área de IT no pueden ser establecidos, el sistema y los datos sensitivos pueden ser determinados en base a niveles de protección requerida para mantener los datos, disponibilidad, integridad y confidencialidad de los sistemas.

La siguiente lista provee una breve descripción de cada objetivo de seguridad y la consecuencia o impacto de no encontrar estas:

- Pérdida de integridad. La integridad de los datos se refieren al requisito de que la información se proteja de la modificación inapropiada
- Perdida de disponibilidad. Si un proceso crítico del sistema no esta disponible a sus usuarios finales, la organización puede verse afectada.
- Pérdida de confidencialidad. La confidencialidad de los sistemas y de los datos se refiere a la protección de la información de descubrimientos no autorizados.

Algunos impactos tangibles pueden ser medidos cuantitativamente en la pérdida de rédito, el costo de reparar el sistema o el nivel de esfuerzo requerido para corregir los problemas causados por la acción de una amenaza.

Otros impactos (por ejemplo la pérdida de la confianza pública, credibilidad, daña los intereses de la organización), no pueden ser medidos en unidades especificas, pero pueden ser calificadas o descritas en términos de impacto alto medio o bajo.

Magnitud del Impacto	Definición del Impacto
ALTO	La ejecución de la vulnerabilidad puede resultar en costos altos, perdidas de activos tangibles y recursos, ocasiona daños o impedir la misión de la empresa, puede causar muertes o personas heridas.
MEDIO	La ejecución de la vulnerabilidad puede resultar en costos, pérdidas de activos tangible, puede violar, dañar o impedir la misión de la empresa.
BAJO	La ejecución de la vulnerabilidad puede resultar en costos bajos, pérdidas de activos tangibles o recursos, puede afectar de alguna forma la misión de la empresa.

FUENTE: Risk Management Guide for Information Technology System (NIST)

Tabla 3.4 Definición de probabilidades

3.1.1.6 Valoración cualitativa vs. Cuantitativa.

En el análisis del impacto, debe considerarse las ventajas y desventajas de la valoración cuantitativa contra la cualitativa. La ventaja principal del análisis de impacto cualitativo es que permite priorizar los riesgos e identifica las áreas, para

inmediatamente dirigirse a las vulnerabilidades, la desventaja es que no proporciona medidas cuantificables especificas de la magnitud del impacto, por esta razón es necesario realizar un análisis costo-beneficio.

3.2 Determinación de requisitos para la elaboración DRP

Para la realización de los planes de recuperación, es necesario determinar los siguientes factores utilizando la metodología del análisis de riesgo que indicaremos a continuación, para posteriormente aplicar en el caso de estudio de la empresa Continental Tire Andina S.A.

3.2.1 Identificación del riesgo y procesos críticos

Para realizar la identificación del riesgo es necesario conocer los recursos y procesos críticos del negocio, los cuales se clasifican se clasifican de la siguiente manera:

- Software
- Hardware
- Equipo de comunicaciones
- Aplicaciones críticas de los sistemas
- Datos e información crítica
- Procesos críticos
- Personal de soporte

Adicionalmente información relacionada con el ambiente operacional del área de IT, entre esta información tenemos:

- Políticas, permisos de usuarios
- Topología de la red

- Respaldos (Backups) que protejan la confidencialidad, integridad y disponibilidad de los datos.
- Seguridad ambiental y físicas del área de IT.

3.2.2 Evaluación del riesgo

El propósito de esta etapa es evaluar el nivel de riesgo de los sistemas y recursos del área de IT, la determinación del riesgo para una particular amenaza/vulnerabilidad puede ser expresada en función de:

- La probabilidad de que se origine una amenaza dada una vulnerabilidad
- La magnitud del impacto de la amenaza provocada por la vulnerabilidad.
- El adecuado plan o controles de seguridad existentes para reducir o eliminar el riesgo.

3.2.2.1 Matriz de Nivel de Riesgo

El riesgo se obtiene multiplicando los valores asignados a la probabilidad y el impacto de la amenaza. En la tabla 3.5 se muestra los niveles de riesgo a los que se les a asignado un valor, para cada nivel de impacto y probabilidad de la amenaza.

Probabilidad de la amenaza	Impacto		
	Bajo (10)	Medio (50)	Alto (100)
Alto (1.0)	10	50	100
Medio (0.5)	5	25	50
Bajo (0.1)	1	5	10

FUENTE: Risk Management Guide for Information Technology System (NIST)

Tabla 3.5 Matriz de Nivel de Riesgo

El valor del riesgo se obtiene de multiplicar cada una de las diferentes celdas de la Matriz de Riesgo. Los valores usados para la multiplicación se obtienen de los

valores asignados al nivel de impacto y la probabilidad. Para el impacto tenemos (Alto (100), Medio (50), Bajo (10) y la probabilidad (Alto (1), Medio (0,5), Bajo (0.1)).

En la tabla 3.6 se representa la definición del nivel de riesgo de acuerdo a la escala establecida.

Escala de riesgo	Definición del rango de riesgo
ALTO	Si el resultado de la matriz de riesgo se encuentra entre 50 y 100. Si una observación es evaluada como de alto riesgo, existe una necesidad grande de tomar medidas correctivas. El sistema como tal puede seguir adelante, pero se debe tomar acciones correctivas para ser puestas en práctica tan pronto sea posible.
MEDIO	Si el resultado de la matriz de riesgo se encuentra entre 10 y 50. Si una observación es evaluada como de riesgo medio, acciones correctivas son necesarias y un plan debe ser desarrollado para integrar estas acciones dentro de un período de tiempo razonable.
BAJO	Si el resultado de la matriz de riesgo se encuentra entre 1 y 10. Si una observación es evaluada como de bajo riesgo, el jefe, el personal y los directores deben decidir si acciones correctivas son necesarias o si se decide aceptar el riesgo.

FUENTE: Risk Management Guide for Information Technology System (NIST)

Tabla 3.6 Definición de la escala de Riesgo

3.2.2.2 Controles para reducir el Riesgo

Durante esta etapa se proporcionan los controles que podrían mitigar o eliminar los riesgos identificados. El propósito de los controles recomendados es reducir el nivel de riesgo en los sistemas datos y recursos del área de IT a un nivel aceptable.

Se debe considerar los siguientes factores para establecer los controles y soluciones alternativas de manera que estos permitan minimizar o eliminar los riesgos identificados:

- La efectividad de las opciones recomendadas (por ejemplo, compatibilidad del sistema)
- Política organizacional
- Impacto operacional
- Seguridad y fiabilidad, etc.

Los controles recomendados son el resultado del proceso de evaluación del riesgo y proporciona la entrada al proceso de mitigación de riesgo. Para determinar que controles se utilizarán es necesario realizar un análisis costo-beneficio.

3.2.2.3 Documentar los resultados

Una vez que la evaluación del riesgo se ha completado (se identificó el origen de las amenazas, vulnerabilidades, se evaluaron los riesgos, y se recomendó los controles apropiados), los resultados deben documentarse en un informe.

Un informe que permita a la organización estar al tanto de los riesgos que se encuentran presentes, de manera que la organización tome decisiones respecto a que políticas se deben implantar y se asigne el presupuesto necesario para reducir el riesgo de acuerdo a los controles recomendados.

3.2.2.4 Información para el análisis de Riesgo dentro de la empresa Continental Tire Andina S.A

Toda la información recolectada para este presente tema de estudio ha sido bajo previa supervisión del área de IT de la empresa para evitar revelar información confidencial o que afecte al Know-How de la empresa Manufacturera de llantas.

Además cabe mencionarse que la información recolectada es en base a entrevistas, visitas en sitio, cuestionarios, revisión de documentos. El riesgo originado por amenazas y vulnerabilidades se determinó en base a la Matriz de Riesgos establecida por el NIST (Instituto Nacional de Estándares y Tecnologías).

La metodología empleada esta descrita dentro del punto 3.4 de este mismo capítulo, en él aplicamos el análisis de riesgo al departamento de Ingenierías de la compañía Continental Tire Andina S.A.

3.2.2.4.1 Identificación de recursos y procesos críticos

Continental

Identificación de recursos y procesos críticos

			Impacto			
Aplicación / Servicio	**Departamento**	**Proceso**	**ALTO**	**MEDIO**	**BAJO**	**NA**
Servidor de aplicaciones SCADA Mixer	Planta Común	Datos históricos y reporte producción (OPC)	x			
		Creación y modificación Recetas		x		
		Operación maquina	x			
Servidor Central para el SIM	Planta General	Reporte Producción (OPC)	x			
		Manejo Inventarios	x			
		Programación Producción	x			
Servidor de Video	Planta General	Monitoreo seguridad física			X	
Servidor SCADA IPC Triplex	Planta Común	Operación maquina	x			
		Creación y modificación Recetas		X		
		Datos históricos y reporte producción	X			
IPC constructoras y Cortadoras	PLT	Operación maquina	x			
		Reporte Producción (OPC)	x			
		Carta de control Calidad		x		
IPC Prensas Zanja H	CVT	Operación de la maquina	x			
		Curvas históricas vulcanización		x		
		Reporte Producción (OPC)	x			
IPC Maquinas Uniformidad	PLT	Operación maquina	x			
		Reportes de Uniformidad		x		
PC Adquisición Datos SIM	Planta General	Reporte Producción (OPC)	x			
		Trazabilidad y Carta control		x		
		Registros de Calidad		X		
PC Adquisición Datos SIM Zanjas	PLT	Registros de Producción varias maquinas	X			
		Curvas históricas vulcanización		X		
		Registro de calidad		x		
IPC Sistemas medición cauchos	PLT / CVT	Datos de calidad de producto		x		
		Reporte de Defectos(OPC)			X	

Tabla 3.7 Aplicaciones y procesos del área de Ing. de Continental

La empresa Continental, cuenta con procesos considerados de alto nivel de impacto a la criticidad de estos representan, en caso de ocurrir un desastre tales procesos no se los puede llevar en formal, por ejemplo el manejo del inventario y la programación de la producción se realiza enteramente con el SIM.

Actualmente no existe manuales de las aplicaciones existentes para poder cargar nuevamente el programa y los drivers en la IPC, algunas aplicaciones fueron desarrollados por externos y no existe respaldo ni documentación sobre esto, por lo que en caso fortuitos se debe contactar al proveedor de la máquina para solucionar una contingencia mayor.

3.2.2.4.1.1 Bases de datos y servidores

En la siguiente Tabla 3.8 se muestra las bases de datos (BDD) disponibles y los servidores o IPC en los cuales están ejecutándose estas aplicaciones:

Servidor/ IPC	Descripción	Base de Datos
IBM Xseries 3650	Servidor del Sistema Integrado de Manufactura	Oracle Enterprise Manager 10 g
HP Proliant 2400	Servidor de aplicaciones del Mixer	Microsoft SQL Server 2000
Beckhoff C6140-1033	IPC Triplex	Microsoft SQL Server 2008
Beckhoff C6140-1040	IPC Constructoras	Microsoft Office Access
Simatic Panel PC 677B	IPC Prensa H	SQL-Protool Pro v6.0

Tabla 3.8 Servidores y Base de Datos

En Continental la base de datos perteneciente al departamento de Ingeniería es la del Sistema Integrado de Manufactura, ya que en ella se programa la producción

diaria, de la planta, el manejo de inventarios, reporte de producción de los 3 Turnos diarios y además que dispone de un modulo de enlace con el ERP de SAP para la generación de pedidos con los proveedores tanto de materias primas como repuestos, etc.

3.2.2.4.1.2 Software instalado

A continuación se detallan en la siguiente cuadro, un resumen del software más relevante instalado en servidores y en IPC que representan de alto impacto para el negocio.

Software Instalado

		Impacto			
ITEM	**DESCRIPCION**	**Alto**	**Medio**	**Bajo**	**NA**
1	OPERATOR Versión 4.2.04.006.8 (11.1.0.8123 Build)	x			
2	Windows Server 2003 Relesase 2 SP2			x	
3	McAfee Virus Scan Enterprise 8.8.0		x		
4	Acronis True Imagen Workstation v9.1			x	
5	McAfree VirusScan Enterprise WorkStation v8.5.0.781	x			
6	Oracle_Oraclient10g_home1		x		
7	TwinCAT OPC DA Server v3.0.0 (Build 40) Beckhoff	x			
8	OPC LabVIEW_DSC Module Runtime System v 7.1 NI	x			
9	Ultra VNC Server			x	

Tabla 3.9 Software instalado en Servidores

El Software considerado como crítico en los servidores es el del Sistema Operativo, Base de Datos y el Antivirus, en caso de existir algún inconveniente se producirá interrupciones en levantar las aplicaciones.

Existe un servidor de cámaras de vigilancia no posee un alto nivel de impacto en la organización, se encuentra instalado otras aplicaciones como utilitarios y archivos de manuales.

Para las computadoras que poseen aplicaciones que corren a nivel de sistema operativo como es TwinCAT que es un SoftPLC, se dispone de imágenes del disco duro y copias virtualizadas de licencias de software para facilitar su recuperación.

3.2.2.4.1.3 Hardware

Dentro de la descripción del Hardware Continental posee un solo servidor para las diferentes aplicaciones del Sistema Integrado de Manufactura, en el cual que el nivel de impacto se especifica de acuerdo a la criticidad que este representa.

En la siguiente tabla hacemos un comparativo con respecto a los otros equipos de la planta:

Continental® **Hardware**

		Impacto			
Hostname Servidores / equipos	**Descripción**	**Alto**	**Medio**	**Bajo**	**NA**
OPERATOR	Servidor para el sistema Integrado de Manifactura.	x			
LINEPC7170	Servidor aplicación SCADA		x		
CP_H1-2	IPC para registro prensa zanja H		x		
IBM_LenovoR61L	PC registro de producción para operador	x			
STC_1121	IPC Beckhoff para control de la maquina	x			
IPC88R9	IPC Beckoff para control de la maquina		x		
MIXER1_2	Servidor para el control del SCADA de los 2 mezcladores	x			

Tabla 3.10 Hardware disponible en Ingenierías

Cabe resaltar que en Continental dispone de una bodega de repuestos donde tenemos en stock los modelos de los computadores industriales, listo para reemplazar las maquinas en caso de fallas o contingencias mayores.

3.2.2.4.1.4 Equipos de comunicación

La empresa Continental Tire Andina, cuenta con los siguientes equipos de comunicación don las diferentes agencias a través de proveedores de internet como es TELCONET o el grupo TV-Cable y enlaces de VPN para soporte y control remoto de las diferentes aplicaciones.

Equipo	Modelo
SWITCH Administrable	CISCO 3750X
ROUTER	CISCO Catalyst 2960 Series SI 48p
SWITCH 24VDC	SIEMENS SCALANCE X206-1
HUB	D Link-DI524

Tabla 3.11 Equipos de comunicaciones

Para el Sistema Integrado de Manufactura, las maquinas que registran la producción comparten la red de datos IT, pero existe ya el proyecto de tener una red dedicada tipo Ethernet Industrial donde la se gestione mejor el manejo de la información y se reduzca la vulnerabilidad que se pueda tener hacia la red IT, sobre todos las aplicaciones financieras que se manejan por la red.

3.2.2.4.1.5 Personal

El personal que forma parte del área de IT y del departamento de Ingenierías responsable de las aplicaciones y servicios es la siguiente:

		Impacto			
Item	**Personal responsable aérea**	**Alto**	**Medio**	**Bajo**	**NA**
1	Jefe de área de IT		x		
2	Analista de Manufactura (Sistema SIM)	x			
3	Programador (proyectos)			x	
4	Administrador de la Red	x			

Tabla 3.12 Personal responsable del área.

Para el área de Ingenierías uno de los cargos considerados como críticos dentro del área, es la persona encargada de monitorear el Sistema Integrado Manufactura, ya que es el responsable de la continuidad del servicio para reporte y monitoreo de la producción.

Otra cargo que posemos mencionar como critico es el Administrador de la red, ya que este servicio es indispensable para el almacenamiento y consulta de la información.

La persona que gestiona la Base de datos para las recetas en las diferentes máquinas posee prioridad media, ya que los PLC almacena la información de parámetros de maquina así como los valores a producir, en algunos casos.

3.2.2.4.2 Identificación de Vulnerabilidades

Estas son las vulnerabilidades que hemos detectado en el área de Ingenierías

3.2.2.4.1.6 Vulnerabilidad de los servidores y Base datos

Dentro de estas podemos enlistar a las siguientes:

a) Se utilizan perfiles de usuarios anteriores, para administrar la aplicación
b) El personal nuevo no cuenta con un manual, ni procedimiento del cambio en las bases de datos y parámetros de máquina.
c) La empresa si realiza la adquisición de actualizaciones para nuevas versiones
d) Se utiliza un único perfil de usuario y no existen ninguna restricción en los permisos de usuario.

Al probar el acceso de archivos compartidos desde la intranet

a) No existe restricción para bajar los archivos
b) El usuario de operación en la maquina local es de tipo administrador
c) Cualquier usuario puede conectarse con aplicación de Escritorio remoto.

3.2.2.4.1.7 Vulnerabilidad en los equipos de comunicaciones

Se ha analizado y se encontró que no se realiza un mantenimiento preventivo, y los equipos debido a la contaminación producida por el proceso de fabricación de neumáticos sufren daños en las tarjetas electrónicas.

En el caso de los switch de FO administrables, se encontró que si existe información referente a la configuración y a el control de direcciones IP usadas en la subred de la intranet de la empresa.

3.2.2.4.1.8 Vulnerabilidad física del área de Ingenierías

Para esto se dialogó con el jefe del departamento y en base a encuestas al personal se pudo determinar lo siguiente:

- El acceso al servidor principal está en el Centro Computo es a través de llaves las cuales solo posee personal de TI.
- No existe registro electrónico de quien ingresa en diferentes horarios a la sala de cómputo.
- En caso de desastre existe una puerta amplia y señalizada por donde evacuar
- Las dimensiones del centro son adecuadas ya que últimamente fue ampliado el espacio físico.
- Se dispone de alarma contra incendios.
- Existe una media dificultad para trasladar equipos en caso de un desastre.
- Las paredes del centro son herméticas y posee un moderno sistema de aire acondicionado.
- No existe bombas de agua en caso de inundación.
- Existe UPS para suplir bajones de tensión y daño en los equipos.

3.2.2.4.3 Identificación de Amenazas

Dentro de las varias amenazas que pueden afectar los recursos y procesos críticos que forman parte del área podemos mencionar las siguientes:

Amenazas Naturales

- Inundaciones (Cercanía a un rio)
- Fuego

- Terremoto
- Erupciones volcánicas.

Amenazas Humanas

- Virus
- Robo
- Sabotaje
- Hacker

Amenazas Ambientales

- Electricidad
- Aire acondicionado
- Proveedor de telecomunicaciones
- Seguridad física
- Fallas de Hardware
- Fallas de Software

3.2.2.4.4 Evaluación del riesgo

Para realizar el análisis del riesgo nos vamos ayudar de la siguiente tabla donde vamos a determinar el impacto de la amenaza que se puede tener en cada una.

En esta tabla estamos considerando los factores más importantes para la evaluación del riesgo que después de determinar la probabilidad de amenazas nos van ayudar para el análisis de resultados.

Continental

Impacto de Amenazas

Amenaza	Servidor de BDD para SIM y aplicación	Servidores SCADA	IPC Control Maquinas	Comunicaciones	Servidor Video
Inundaciones	ALTO	ALTO	ALTO	MEDIO	MEDIO
Fuego	ALTO	ALTO	ALTO	MEDIO	MEDIO
Terremotos	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO
Erupciones volcánicas	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO
Robo	MEDIO	BAJO	BAJO	MEDIO	MEDIO
Aire acondicionado	MEDIO	MEDIO	ALTO	BAJO	BAJO
Electricidad	MEDIO	MEDIO	MEDIO	MEDIO	BAJO
Proveedores de comunicaciones	MEDIO	BAJO	BAJO	MEDIO	BAJO
Fallas de Hardware	ALTO	ALTO	ALTO	MEDIO	MEDIO
Fallas de Software	ALTO	ALTO	ALTO	BAJO	BAJO
Virus (USB)	ALTO	ALTO	ALTO	BAJO	MEDIO
Hacker	MEDIO	BAJO	BAJO	BAJO	MEDIO
Sabotaje	ALTO	ALTO	ALTO	BAJO	BAJO
Partículas de materia prima	BAJO	ALTO	ALTO	MEDIO	BAJO
Seguridad Física	MEDIO	MEDIO	MEDIO	BAJO	MEDIO

Tabla 3.13 Impacto de las amenazas

La empresa se encuentra ubicada junto al rio Machángara, por lo que para la situación de nuestra empresa el riesgo de Inundaciones es muy alta, también hay que resaltar que el mayor reporte que hemos registrado por infección de virus informáticos es debido al uso indebido de los dispositivos de almacenamiento externo USB, que introducen virus a la red.

La probabilidad de que las amenazas identificadas lleguen a afectar a los diferentes equipos dentro del departamento se detalla en la siguiente Tabla 3.14.

Continental

Probabilidad de Amenazas

Amenaza	Servidor de BDD para SIM y aplicación	Servidores SCADA	IPC Control Maquinas	Comunicaciones	Servidor Video
Inundaciones	MEDIA	ALTO	ALTO	MEDIO	MEDIO
Fuego	BAJO	BAJO	MEDIO	BAJO	BAJO
Terremotos	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO
Erupciones volcánicas	BAJO	BAJO	BAJO	BAJO	BAJO
Robo	BAJO	BAJO	BAJO	BAJO	BAJO
Aire acondicionado	MEDIO	MEDIO	ALTO	BAJO	BAJO
Electricidad	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO
Proveedores de comunicaciones	MEDIO	BAJO	BAJO	MEDIO	BAJO
Fallas de Hardware	BAJO	ALTO	ALTO	BAJO	MEDIO
Fallas de Software	BAJO	BAJO	BAJO	BAJO	BAJO
Virus (USB)	MEDIO	ALTO	ALTO	BAJO	MEDIO
Hacker	MEDIO	BAJO	BAJO	BAJO	MEDIO
Sabotaje	BAJO	BAJO	BAJO	BAJO	BAJO
Partículas de materia prima	BAJO	ALTO	ALTO	MEDIO	MEDIO
Seguridad Física	MEDIO	MEDIO	MEDIO	MEDIO	MEDIO

Tabla 3.14 Probabilidades de las amenazas

Análisis de Resultados

Dentro de las ***amenazas naturales*** podemos destacar que dentro del análisis que las inundaciones posee una probabilidad ALTA, ya que por la ubicación de la empresa junto a un rio es posible que se de este contingente, por lo que es necesario tener un buen sistema de drenaje, y todos los equipos con bases elevadas para mitigar hasta salvaguardar los equipos.

En cuanto a las ***amenazas humanas***, según el análisis podemos ver que la probabilidad de Virus es muy ALTA, ya que al tener computadores para el registro de producción en cada máquina, los operadores hacen mal uso de los USB para conectar y cargar reproductores de música, lo que produce infecciones, aunque se

dispone de un antivirus actualizada, y se ha implementado el bloqueo de USB para mitigar la infección. La probabilidad de Robo y sabotaje por hacker se mantiene baja, además de ser una empresa que cuenta con una área cerrada donde esta las instalaciones con guardianía privada.

Dentro de las ***amenazas ambientales*** tenemos que la falla del sistema de aire acondicionado puede ser considerada como una amenaza, aunque tiene una probabilidad media, ya que se instalaron recientemente equipos nuevos y se tiene ambiente cerrado y personal de mantenimiento preventivo.

En cuanto al servicio de energía eléctrica, esta es considerada media, ya que la empresa cuanta con un buen sistema de UPS, un grupo de generadores para suplir alimentación a planta y a los centros de cómputo, pero siempre es un problema la variación de tensión en los cortes y se presentan daños en el hardware.

Una vez identificados estos indicadores vamos a proceder a determinar la matriz de evaluación de riesgo, esta se obtiene multiplicando el impacto de probabilidad de ocurrencia por cada amenaza.

Los valores usados para la multiplicación son los descritos en la Tabla 3.5, de acuerdo a esta tabla se obtuvieron los siguientes valores representados en la siguiente Tabla.

Continental

Matriz de Evaluación de Riesgo

Amenaza	Servidor de BDD para SIM y aplicación	Servidores SCADA	IPC Control Maquinas	Comunicaciones	Servidor Video
Inundaciones	50	100	100	25	25
Fuego	10	10	50	5	5
Terremotos	25	25	25	25	25
Erupciones volcánicas	5	5	5	25	5
Robo	5	1	1	5	5
Aire acondicionado	25	25	100	1	1
Electricidad	25	25	25	25	5
Proveedores de comunicaciones	25	1	1	25	1
Fallas de Hardware	50	100	100	5	25
Fallas de Software	10	10	10	1	1
Virus (USB)	50	100	100	1	1
Hacker	25	5	1	1	25
Sabotaje	10	10	10	1	1
Partículas de Negro Humo	1	100	100	25	5
Seguridad Física	25	25	5	5	25

Tabla 3.14 Matriz de evaluación de riesgo

3.2.2.4.5 Controles para mitigar el riesgo

Dentro de los controles preventivos que permitirán minimizar o disminuir de alguna forma el riesgo producido por el impacto de las amenazas que podrían presentarse, entre los controles recomendados tenemos:

a) Verificar periódicamente el sistema de aire acondicionado en el centro de computo
b) Evaluar periódicamente el sistema de enfriamiento de IPC instalados en planta para evitar fallas por sobre-temperatura en los equipos.

c) Instalar periódicamente las actualizaciones de Antivirus ya sea de forma automática por medio de la red, o en sistema aislados por medio del Update manual utilizando un dispositivo externo previamente vacunado.
d) Adquirir herramientas o dispositivos de seguridad que ofrezcan protección contra programas maliciosos y generen una alarma cuando se sospecha de una actividad dudosa.
e) Difundir las normas y políticas existentes, para disminuir en forma sustancial el mal uso de los recursos informáticos y el acceso de posibles hacker.
f) Debe verificarse que el registro de visitantes al área sea llenado para tener control de que personal ya sea soporte, limpieza, técnicos, etc., han ingresado.

3.3 Elaboración de normas y políticas

Dentro de las normas y políticas que podemos mencionara en base a las mejores prácticas, teniendo en cuenta que el principal paso para el desarrollo del DRP, es un correcto análisis de Riesgo, determinando todas las posibles amenazas y vulnerabilidades alineados con los objetivos del departamento de Ingenierías de la Empresa Continental Tire Andina S.A. Dentro de estas podemos mencionar a los siguientes:

3.3.1 Implementación de controles para reducir el riesgo

Se debe aplicar controles preventivos que permitan minimizar o disminuir de alguna forma el riesgo producido por el impacto de las amenazas que podrían presentarse en el área de IT, entre los controles tenemos:

a) Chequeo periódico de las condiciones ambientales, por ejemplo: Mantenimiento adecuado del Aire Acondicionado para evitar partículas en los equipos que causan daños en el sistema eléctrico y electrónico.
b) Revisar las condiciones de infraestructura de Obras Civil en el lugar donde se encuentran ubicados los equipos
c) Adquirir todos las actualizaciones de software en servidores
d) Actualizar versiones de antivirus
e) Instalar dispositivos de seguridad física adecuados al acceso de cuarto de equipos
f) Adquirir herramientas o dispositivos de seguridad de información que ofrezca protección contra programas maliciosos
g) Implementar bitácoras de registro de visitantes
h) Crear registro de Control de cambios dentro de las configuraciones

Estas dentro de los principales controles que se deben tomar en cuenta para mitigar las amenazas y vulnerabilidades dentro de los centros de cómputo y servidores en las areas de IT de las empresas.

3.4 Desarrollo de metodologías

El análisis de riesgo es el primer paso en la metodología de evaluación del riesgo. Este análisis permite identificar las amenazas y vulnerabilidades a las que está expuesta el Área de Ingenierías dentro de la Empresa Continental. Adicionalmente este análisis permite establecer los controles apropiados para mitigar o eliminar los riesgos identificados a un nivel aceptable.

La metodología de análisis del riesgo se detalla a continuación:

a) Identificación del Riesgo
    - Identificación de amenazas

- Identificación de vulnerabilidades
- Análisis de control
- Determinación de la probabilidad
- Análisis de impacto

b) Identificación del recursos y procesos críticos
c) Evaluación del riesgo
   - Controles para reducir el riesgo
   - Documentación de resultados

3.5 Determinación del alcance del DRP

El propósito del análisis de riesgo está dado por tres objetivos básicos:

- Identificar los procesos de negocio y asociarlos con los requerimientos de los recursos de la infraestructura IT referentes a datos, aplicaciones, sistemas y redes que son usados para la entrega de los procesos de negocio o en este caso de Ingeniería dentro de la empresa Continental y Tire Andina S.A.
- Identificar las amenazas existentes en los procesos de negocio y los recursos de infraestructura.
- Priorizar los procesos del negocio de acuerdo a la cantidad, tiempo susceptible y criticidad.
- Definir estrategias de eliminación de riesgos y minimizar el impacto de los riesgos que no puedan ser eliminados.

Capítulo 4

Elaboración de planes BIA

CAPITULO 4. ELABORACION DE PLANES BIA

4.1 Introducción

El Análisis del Impacto en el Negocio (BIA), permite identificar los requerimientos de los sistemas, procesos y recursos críticos para luego con esta información determinar las prioridades y definir las posibles estrategias de recuperación, las que proporcionan medios para restaurar las operaciones del SIM rápida y eficazmente luego de que se produzca una interrupción en el servicio o daño provocado por un desastre.

El tipo de criterio para evaluar el impacto puede incluir: servicio al cliente, operaciones internas, estatutos legales y financieros.

4.2 Propósito del Análisis de Impacto en el Negocio

El Análisis de Impacto en el Negocio es un paso importante en el desarrollo del Plan de Recuperación de Desastres (DRP). El BIA permite identificar los recursos y procesos críticos para determinar el impacto, tiempo de interrupción y prioridades de recuperación en el negocio.

El propósito del Análisis de Impacto en el Negocio (BIA), es relacionar los recursos específicos con los procesos críticos de los sistemas, en base a esta información se determinan las consecuencias que se presentan en caso de producirse una interrupción en los recursos del Área IT.

Los resultados del Análisis de Impacto en el Negocio (BIA) deben incorporarse apropiadamente en el desarrollo de estrategias de recuperación que forman parte del Plan de Recuperación de Desastres (DPR).

Algunos de los beneficios que el Análisis de Impacto en el Negocio (BIA) proporciona al negocio son los siguientes:

- Permite identificar, priorizar sistemas y aplicaciones críticas que dan apoyo a las funciones u operaciones del negocio.
- Permite identificar y definir las prioridades necesarias para la recuperación.
- Determina el costo del tiempo que el negocio pasa fuera de servicio para definir un presupuesto razonable para la recuperación de desastres.
- Proporciona los datos necesarios para representar a la Gerencia y poder justificar el presupuesto destinado a la recuperación de desastres.

4.2.1 Identificación De Los Recursos Críticos Del Área IT

Los sistemas del Área IT pueden ser muy complejos, con numerosos componentes, interfaces y procesos, lo que implica diferentes perspectivas en la importancia de los servicios del sistema.

El primer paso del Análisis de Impacto en el Negocio (BIA), es evaluar los sistemas del Área IT para determinar las funciones críticas del sistema y los recursos específicos. Dos actividades usualmente son necesarias para complementar este paso:

- El Coordinador del Plan de Recuperación de Desastres (DRP), debe identificar y coordinar con el personal de contacto interno y externo asociados con el sistema para determinar la manera que ellos dependen o dan soporte a los sistemas del Área IT. Además de identificar al personal de contacto, es importante incluir las organizaciones que proporcionan o reciben los datos del sistema, así como también al personal de soporte de cualquier sistema interconectado. El coordinador debe permitir al Administrador del Sistema determinar el rango de apoyo necesario para el

sistema en el que se debe incluir los requerimientos técnicos, operacionales y de seguridad.

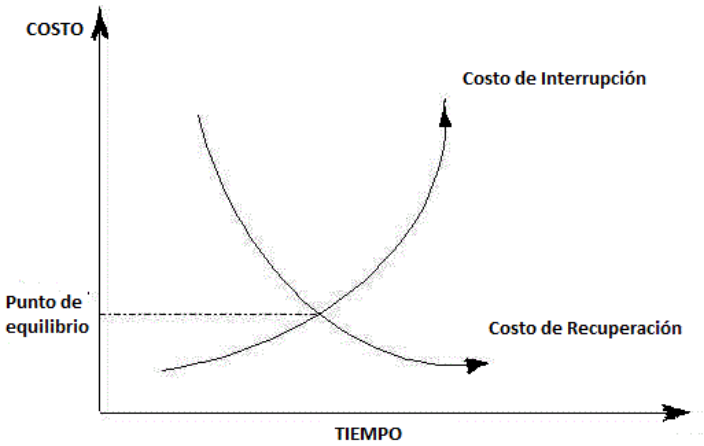
- El coordinador del Plan de Recuperación de Desastres (DRP) debe evaluar el sistema para unir estos servicios críticos a los recursos del Área IT. Este análisis identificara los requerimientos de infraestructura referente a los equipos específicos, tales como: routers, servidores de aplicaciones, y servidores de autentificación, que son considerados críticos. Sin embargo, el análisis puede determinar que recursos son seguros, por ejemplo: una impresora o servidor de impresión no son necesarios como apoyo de los servicios críticos identificados.

4.2.2 Identificación del Impacto y Tiempo de Interrupción aceptable.

Se debe analizar los recursos críticos identificados en el paso anterior y determinar el/los impacto(s) en las operaciones IT, en el caso de que un recurso no se encuentre disponible por una interrupción o daño. El análisis debe evaluar el impacto de la interrupción de dos maneras.

- Los efectos de una interrupción pueden rastrearse con el tiempo. Esto permitirá al Coordinador del Plan de Recuperación de Desastres (DRP), identificar el tiempo máximo permitido de interrupción del recurso, antes que se produzca un daño potencial.
- Los efectos de la interrupción pueden ser rastreados por los recursos y personas relacionadas con el sistema, de forma que se identifique cualquier efecto de cascada que afecte a otros procesos que dependen del sistema.

El Coordinador del Plan de Recuperación de Desastres (DPR), debe determinar el punto óptimo para recuperar el sistema IT equilibrado el costo del sistema inoperable contra el costo de los requeridos para restaurar el sistema.



FUENTE: Contingency Planning Guide for Information Technology Systems (NIST)

Fig. 4.1 Equilibrio entre Costo de Interrupción y Costo de Recuperación

En la Fig. 4.1 se muestra el punto de unión de las dos líneas el cual define el tiempo que el negocio puede detenerse antes de que el sistema se ha interrumpido completamente.

4.2.3 Identificación de Controles Preventivos

Como se indicó anteriormente, el Análisis de Impacto en el Negocio (BIA) puede proporcionar al Coordinador del Plan de Recuperación de Desastres (DRP), información vital con respecto a la disponibilidad del sistema y requisitos de recuperación. En algunos casos, puede mitigarse o eliminarse los impactos de la interrupción identificados en el Análisis de Impacto en el Negocio (BIA) a través de controles preventivos que pueden detectar, descubrir, y/o reducir los impactos en el Área IT.

Existe una amplia variedad de controles preventivos que están disponibles, dependiendo del tipo de sistema y configuración; sin embargo, algunas medidas comunes se listan a continuación:

- Suministros de Poder Continuo (UPS), para proporcionar energía a corto plazo a todos los componentes del sistema (incluyendo medioambiente y controles de seguridad).
- Gasolina o diesel para proveer energía a los generadores que proporcionaran energía eléctrica a largo plazo.
- Sistemas de Aire Acondicionado con la capacidad de evitar fallas en los equipos.
- Sistemas de Supresión de Fuego.
- Detectores de fuego y humo.
- Sensores de agua en el Centro de Cómputo colocados en el techo y suelo.
- Lonas plásticas que pueden desenrollarse para evitar daños en los equipos del Área IT.
- Interruptor de emergencia maestro para cerrar sistemas.
- Almacenamiento fuera de sitio de medios de respaldo, registros no electrónicos y documentación del sistema.
- Controles técnicos de seguridad, como la administración de claves criptográficas y controles de acceso de menor privilegio.
- Respaldos frecuentes.

Se debe documentar en el Plan de Recuperación de Desastres (DRP), los controles preventivos que se implante en el Área IT, adicionalmente es necesario entrenar al personal asociado con el sistema sobre cómo y cuándo usar los controles. Estos controles deben mantenerse en buena condición para asegurar su efectividad en una emergencia.

4.3 Objetivo posibles estrategias de recuperación de desastres

Las estrategias de recuperación proporcionan medios para restaurar las operaciones IT rápida y eficazmente después de que se produzca una interrupción del servicio, estas estrategias deben dirigirse a la recuperación de los procesos y recursos críticos del negocio de acuerdo a los niveles de impacto y tiempo aceptable de la interrupción identificados en el análisis de Impacto en el Negocio (BIA).

Las estrategias de recuperación pueden incluir una combinación de métodos entre los cuales tenemos: controles preventivos, tecnologías y técnicas de recuperación, que se complementan entre sí para proporcionar la capacidad de recuperación, sobre la gama de incidentes que se presentan dentro del Área IT y afectan las operaciones normales del negocio. Además para el desarrollo de las estrategias es necesario considerar ciertos aspectos tales como: costos, tiempo aceptable de interrupción y seguridad.

Para definir las estrategias de recuperación de desastres se debe considerar lo siguiente:

- Métodos de respaldo (Backup)
- Sitios alternos.
- Reemplazo de Equipos.
- Roles y responsabilidades.
- Costos

4.3.1 Métodos de Respaldos (Backup)

La información del sistema, Bases de Datos y archivos de los usuarios deben respaldarse regularmente. Las políticas establecidas en el Área IT, deben especificar la frecuencia de respaldos (Ejemplo: diario o semanal, incremental o

Full), basados en la criticidad de los datos y la frecuencia que la nueva información es ingresada. Los tipos de frecuencias de respaldos se detallan a continuación:

- **Full.** Un respaldo (full backup) graba en un medio específico (Tape) todos los archivos del disco o de una carpeta seleccionada, la localización de un archivo o grupo de archivos, es simple. Sin embargo, el tiempo requerido para realizar un full backup puede ser largo. Además los full backups frecuentemente no cambian ocasionando requerimientos innecesarios de medios de almacenamiento.
- **Incremental.** Un respaldo incremental graba los archivos que se crearon o se cambiaron desde el último respaldo, sin tener en cuenta el tipo de respaldo utilizado. Los respaldos incrementales utilizan de manera más eficaz los medios de almacenamiento, y los tiempos de respaldo son reducidos. Sin embargo, para recuperar un archivo desde un respaldo incremental, puede requerirse medios diferentes.
- **Diferencial.** El respaldo diferencial graba archivos que se crearon o modificaron desde el último full backup. El respaldo diferencial tarda menos tiempo que el full backup, la restauración puede requerir menos medios que un respaldo incremental porque solo se necesitaría los medios de full backup y el último diferencial. La desventaja del respaldo diferencial es que tarda más tiempo en completarse debido a la cantidad de datos a recuperar desde el último full backup.

Las políticas de respaldos de los datos establecidas en la organización deben designar la localización de los datos almacenados, la convención de nombres, frecuencia de rotación del medio, y métodos para transportar los respaldos fuera del Sitio Primario. Los datos pueden almacenarse en discos magnéticos, tape o discos ópticos (como discos compactos CDs).

El método específico escogido para realizar los respaldos debe estar basado en el sistema, datos disponibles y requerimientos de integridad. Estos métodos de respaldo incluyen: Electronic Vaulting, Disk Mirroring y Data Tape Backup.

Para seleccionar el método de almacenamiento fuera de sitio es necesario considerar los siguientes criterios:

- **Área Geográfica.** Específica la distancia que existe entre la organización y el sitio probable donde se almacenan los respaldos, en caso de presentarse un desastre este podría afectar tanto a la organización como al Sitio Alterno dependiendo de la distancia.
- **Accesibilidad.** Establece el tiempo necesario para la recuperación de los datos desde el medio de almacenamiento.
- **Seguridad.** Las seguridades para el almacenamiento de los datos deben considerar dos puntos: la facilidad de almacenamiento y la confidencialidad del empleado que realiza este proceso. El empleado debe reunir los datos sensibles y los requisitos de seguridad para el almacenamiento.
- **Ambiente.** Estructura y condiciones ambientales para facilitar el almacenamiento (Por ejemplo: temperatura, humedad, prevenciones de fuego, etc).
- **Costos.** Costos operacionales y de servicio de recuperación de desastres.

Estrategia	Descripción	Ventajas	Desventajas	Costo
Tradicional Respaldo en Cinta	Proceso manual de copiar los datos desde el disco duro al medio utilizando para el respaldo	Tecnología simple de implementar, múltiples dispositivos/software disponible.	Transporte manual y almacenamiento riesgoso y erróneo. Tiempo potencialmente largo en caso de restauración.	Bajo a medio

	(tape) y transportarlo a un sitio seguro.			
Respaldo – ElectronicTape Vault	Copiar los datos desde el disco a un sistema de Tape remoto a través de un enlace WAN	Los datos están disponibles en corto tiempo, los servicios son estandarizados, los enlaces WAN se exponen a riesgos se reducen los errores de los métodos manuales.	Los enlaces WAN pueden introducir perdidas en tiempos de respuesta dentro del proceso de respaldo dependiendo del proveedor de almacenamiento, puede ser difícil restaurar los datos, utilizan un tiempo potencialmente largo.	Medio a Alto

Estrategia	Descripción	Ventajas	Desventajas	Costo
Disk Mirroring	Copiar los datos escritos en un disco o arreglo de discos a un segundo disco o arreglo de discos a través	Se restaura instantáneamente, el acceso a los datos posiblemente depende de la disponibilidad del enlace WAN y la	El enlace WAN puede perdida en los tiempos de respuesta dentro de las operaciones del sistema de producción, algunos sistemas	Alto

	de un enlace WAN	sincronización del primero y el arreglo de espejos.	de mirroring reducen la ejecución del sistema de producción; los errores lógicos pueden ser replicados desde el original al conjunto de datos del disco espejo.	

FUENTE: Disaster Recovery Planning (NIST)

Tabla 4.1 Respaldo de datos y alternativas de restauración.

4.3.2 Sitios Alternos

Se debe considerar para el Plan de Recuperación de Desastres (DRP), las interrupciones con efectos a largo plazo. De forma que en el plan se debe incluir una estrategia para recuperar las operaciones y funciones del sistema por un periodo extendido. En general tres tipos de sitios alternos están disponibles:

- Sitio especifico de operaciones propio de la organización.
- Un acuerdo reciproco con una entidad interna o externa.
- Facilidad de arrendamiento comercial.

Sin tener en cuenta el tipo de Sitio Alterno escogido, lo que se pretende es brindar la disponibilidad y el apoyo para el funcionamiento de los sistemas, esto se define en el Plan de Recuperación de Desastres (DRP). Los tres tipos de Sitios Alternos pueden clasificarse en lo referente a su prontitud operacional. Basados en este factor, los sitios identificados son:

- Cold Sites.
- Warm Sites.
- Hot Sites.
- Mobile Sites.
- Mirrored Sites.

4.3.2.1 Cold Sites

Los Cold Sites proporcionan el adecuado espacio e infraestructura (Sistema eléctrico, conexiones de telecomunicaciones, y controles ambientales) para dar soporte a los Sistemas del Area IT. Cabe mencionar que este sitio no cuenta con equipos tales como: servidores, routers, equipos de comunicación, etc., y normalmente no cuenta con equipos de oficina como son: teléfonos, fax o copiadora.

La organización que utilice un Cold Site debe ser la responsable de proporcionar e instalar el equipo necesario y habilitar las comunicaciones. La activación del Centro Alterno puede llevar semanas.

4.3.2.2 Warm Sites

Los Warm Sites son espacios de oficina parcialmente provistos que cuentan con algunos o todos los equipos y recursos necesarios para el funcionamiento de un Centro Alterno tales como: hardware software, telecomunicaciones, y sistema eléctrico, pero sin ordenador principal a menudo este sitio se encuentra equipado con una CPU de menor capacidad.

El Warm Site es mantenido en un estado operacional preparado para recibir a los sistemas que deben ser localizados en un Sitio Alterno. En muchos casos. Un Warm Site puede estar funcionando con otro sistema, en caso de activarse el Plan de Recuperación de Desastres, las actividades normales son desplazadas temporalmente para ubicar el sistema dañado.

El supuesto que respalda el concepto de Warm Site es que, en una situación de emergencia, el ordenador principal se puede obtener rápidamente (siempre que sea un modelo de uso común).

Después de la instalación de los componentes necesarios, el Sitio Alterno puede ser considerado listo para el servicio en cuestión de horas; sin embargo la ubicación e instalación del CPU principal y de otras unidades faltantes puede llevar días o semanas.

4.3.2.3 Hot Sites

Los Hot Sites son oficinas clasificadas según su tamaño para poder dar soporte apropiadamente a los requerimientos de los sistemas, además tienen un hardware configurado con los requisitos del sistema, posee una infraestructura y personal de soporte. Los Hot Sites proveen soporte 7x24 (7 días a la semana 24 horas al día). El personal del Hot Site empieza a prepararse para recibir al sistema en cuanto se les notifique que el Plan de Recuperación de Desastres se ha activado.

4.3.2.4 Mobile Sites

Son sitios móviles autónomos y transportables a menudo se encuentran en un tracto-remolque. Los Mobile Sites proveen un servicio específico de telecomunicaciones y equipo necesario para reunir los requerimientos del sistema. Estos se encuentran disponibles para el arriendo a través de los vendedores comerciales.

En la mayoría de los casos puede ser una solución de recuperación viable, se debe diseñar los sitios móviles en coordinación con el vendedor y establecer un contrato de nivel de servicio entre las dos partes. Esto es necesario porque el tiempo para configurar el sitio móvil puede ser extenso, y si no se cuenta con una previa coordinación, el tiempo para la entrega el sitio móvil puede exceder el tiempo de interrupción de los sistemas del Área IT

4.3.2.5 Mirrored Sites

Los Mirrores Sites son sitios totalmente redundantes, la información es reflejada en tiempo real. Los Mirrored Sites son sitios idénticos al Sitio Primario en los aspectos técnicos, porque proporcionan un alto grado de disponibilidad, además los datos se procesan y almacenan en el Sitio Primario y en el Sitio Alterno de forma simultánea. La organización es la que se encarga de diseñar, construir, mantener y operar los Mirrored Sites.

Estos centros de procesamiento están totalmente configurados y listos para operar en un plazo de pocas horas. El equipamiento y el software de los sistemas deben ser compatibles con la instalación primaria de la que actúa como respaldo, las únicas necesidades adicionales son: el personal, programas y archivos.

Para seleccionar el Sitio Alterno más adecuado para la organización se considera las diferencias que implican el tiempo y el costo de las cinco opciones de Centros Alternos. Los criterios de selección del sitio Alterno se detallan a continuación:

- El Mirroring Site es la opción más costosa, pero asegura casi la disponibilidad del 100 por ciento.
- Los Hot Sites son costosos de mantener; sin embargo se justifican los costos altos en aplicaciones críticas, además pueden requerir tiempo

sustancial para adquirir e instalar el equipo necesario. Cuando se planifica correctamente, la cobertura de seguros se compensara sobre la base de los costos incurridos por utilizar este tipo de instalación.

- En ocasiones, se puede entregar un sitio móvil a la localización deseada dentro de 24 horas.
- El Coordinador debe asegurar la seguridad del sistema, la administración, controles operacionales, y controles técnicos compatibles con el Sitio Alterno.
- Las organizaciones pueden poseer un Sitio Alterno o mantener sitios en base a contratos con empresas externas. Si se llega a un acuerdo en el que el vendedor provea un sitio es necesario tener en cuenta los siguientes aspectos: tiempo adecuado para realizar las pruebas, lugar de trabajo, requisitos de seguridad, hardware, telecomunicaciones, servicios de apoyo, y días de recuperación (cuanto tiempo la organización puede ocupar el espacio durante el periodo de recuperación) estas observaciones deben negociarse y claramente declararse en el contrato.
- Hay que tomar en cuenta que varias organizaciones pueden llegar a un acuerdo con el mismo vendedor para utilizar el mismo Sitio Alterno; de manera que si se produce un desastre este puede afectar a muchas organizaciones, razón por la cual el Sitio Alterno puede ser incapaz de acomodar a todos los clientes de forma simultánea, en este caso se debe negociar la prioridad que cada organización tendrá.

4.3.3 Reemplazo de Equipo

Si el Área IT está dañada, destruida o el Sitio Primario está inhabilitado, el hardware y software necesario debe ser activado rápidamente en un Sitio Alterno. Existen tres grandes estrategias para el reemplazo de equipos. Al seleccionar la

estrategia más apropiada, se debe considerar que la disponibilidad de transporte se puede limitar o detener temporalmente en caso de un desastre catastrófico.

- **Contratos con Proveedores.** En el desarrollo del Plan de Recuperación de Desastres (DRP), se debe considerar los Contratos de Nivel de Servicio (SLA), que proveen los vendedores en cuanto a hardware, software y soporte en caso de emergencia. El Contrato de Nivel (SLA), debe especificar que tan rápidamente el proveedor debe responder después de que se lo ha notificado, además debe constar el estado de prioridad que recibirá la organización en caso de que un desastre catastrófico involucre a múltiples clientes del proveedor. Los detalles de las negociaciones en el Contrato de Nivel de Servicio (SLA) debe adjuntarse con el Plan de Desastres (DRP).
- **Inventario de Equipos.** El equipo requerido puede estar comprado o comprarse de antemano y almacenarse en un sitio seguro fuera del Sitio Primario, como es el caso de un Sitio Alterno donde las operaciones de recuperación tendrán lugar (Hot Site, Mobile Site, etc.) u otro sitio donde se almacene los equipos y entonces se envíe al Sitio Alterno en caso que un desastre afecte al Sitio Primario de la organización. Esta solución presenta un inconveniente que se refiere a que los equipos que se adquieran podrían poner obsoletos o impropios con el tiempo.
- **Equipo Existente Compatible.** Los equipos frecuentemente usados en contratos Hot Sites pueden usarse por la organización afectada mediante acuerdos recíprocos, de manera que los equipos compatibles estarán disponibles para el uso en caso de desastre.

4.3.4 Roles y responsabilidades

Una vez seleccionadas las estrategias de recuperación de los sistemas y recursos del Área IT, el Coordinador del Plan de Recuperación de Desastres debe designar

el personal de recuperación y los equipos apropiados para implementar las estrategias. Cada persona que forma parte de los equipos de recuperación de la organización debe estar entrenada y preparada para trasladarse en caso de que una interrupción requiera la activación del Plan.

El personal de recuperación de desastres puede estar asignado a uno o varios equipos específicos que responderán al evento y se encargaran del proceso de recuperación y de devolver el normal funcionamiento de los sistemas.

Los equipos requeridos para la recuperación después de que se ha presentado una interrupción o desastre en el Área IT, se basan en los sistemas y recursos afectados. El tamaño de los títulos y el diseño de jerarquía de los equipos dependen de la organización. A continuación se listan algunos grupos que pueden formar parte del Plan de Recuperación de Desastres:

- Equipo de valoración del daño
- Equipo de software.
- Equipo de Recuperación de Servidores (por ejemplo, Web Server, Servidor de Correo Electrónico, etc.).
- Equipo de recuperación LAN/WAN.
- Equipo de Recuperación de Base de Datos.
- Equipo de operaciones de la Red.
- Equipo de Recuperación de Aplicaciones
- Equipo de pruebas.
- Equipo de telecomunicaciones.
- Equipo de salvamento de Hardware.

Cada equipo tiene un líder que dirige el funcionamiento adecuado del equipo, además el líder se encarga de la presentación, dirección y el enlace con otros líderes de los equipos. El líder del equipo comunica la información a los miembros

del equipo y aprueba cualquier decisión que debe tomarse dentro del equipo. Es necesario contar con una persona de reemplazo designada para actuar como líder en el caso de que el líder primario no se encuentre disponible.

Para la mayoría de las organizaciones, un Equipo de Dirección es necesario para proporcionar una guía global en el caso de ruptura del sistema, emergencia o desastre inminente. El Equipo de Dirección también facilita la comunicación entre otros equipos, dirige las pruebas y los ejercicios del Plan de Recuperación de Desastres.

4.3.5 Costos

El Coordinador del Plan de Recuperación de Desastres debe asegurarse que las estrategias escogidas pueden llevarse a cabo eficazmente con el personal y los recursos financieros disponibles.

El costo de cada estrategia seleccionada debe ser evaluado sobre la base de las limitaciones del presupuesto. El coordinador es la persona encargada de determinar los gastos que implica la recuperación de desastres, las cuotas del contrato del Sitio Alterno y considerar otros gastos. El presupuesto debe ser suficiente para abarcar software, hardware, transporte, embarque, pruebas del Plan de Recuperación de Desastres, horas laboradas y otros servicios contratados. Razón por la cual es necesario realizar un análisis de costo beneficio para identificar la estrategia de recuperación más óptima.

4.4 Organización del BIA

Para realizar el análisis de impacto en el negocio, es necesario seguir una metodología al igual que lo realizamos en el análisis del riesgo, que empieza por la

identificación de recursos críticos en el área, donde hacemos una correlación entre los equipos, aplicaciones, usuarios que administran e incluso los proveedores, una vez determinado esto se procede a determinar la identificación del impacto y tiempo de interrupción aceptable.

Identificados los procesos y tabulados en tablas, se procede al desarrollo de las prioridades de recuperación para los procesos críticos, esto en base a un esquema como es ALTO, MEDIO, BAJO, todos los procesos que tenga una prioridad alta exige un control preventivo, que permitirán de alguna manera mitigar el riesgo que representan.

4.5 Plan de acción en el Análisis del Impacto en el Negocio (BIA) dentro de la empresa Continental Tire Andina S.A

El Análisis de Impacto en el Negocio permite identificar los procesos, aplicaciones y recursos críticos del Área de IT de Continental, mediante este análisis es posible determinar las prioridades y definir los tiempos mínimos de recuperación requeridos para cada aplicación, posteriormente con esta información se definen las posibles estrategias de recuperación que se utilizarán después de que se ha producido una interrupción o desastre.

Para este estudio se utilizó una guía de formato facilitado por la empresa que permite obtener información sobre los diferentes aspectos referentes a los sistemas y procesos que forman parte del Área del Departamento de Ingenierías.

4.5.1 Identificación de recursos críticos

Los recursos críticos con los que cuenta el departamento se clasifican de la siguiente manera en Hardware, Software, Equipos de comunicación y Aplicaciones, estos recursos se describen en la siguiente tabla:

Hardware:
• IBM Xseries 3650 • HP Compaq 6200 • Beckhoff C6140-1033 • SIEMENS Simatic Panel PC 677B • IBM Lenovo R61i
Software:
• Windows Server 2003 Release 2 • SQL Anywhere Studio 9 • SQL Server 2000 • McAfee Virus Scan Enterprise 8.8.0 • OraClient 10g • OPC LabVIEW DSC Module Runtime System v7.1 • TwinCAT OPC DA Server v3.0
Aplicaciones:
• Operator Systems V4.2 • Protool Pro RT V6.0 • Simatic WinCC Profesional_SCADA • Wonderware Intouch
Equipos de Comunicación:
• Switch Administrable CISCO Catalyst 2960 Series SI • Switch Administrable DLink DES-3028 • Switch SIEMENS Scalance X206-1

Tabla 4.2 Recursos críticos

Dentro del área de IT, cuenta con personal interno y además existe una persona de IT que trabaja en el departamento de Ingenierías que brinda soporte directo para cualquier eventualidad del Sistema Integrado de Manufactura, además existe personal externo que brinda soporte del enlace y soporte de servidores principales, esto lo podemos apreciar en la siguiente tabla.

Personal Área de Ingenierías y IT		
Cargo	**Aplicaciones**	**Funciones**
Jefe área de IT	Base de Datos ORACLE-Informix	Administración general SIM y ERP (SAP)
Administrador de la red		Administrar la red, soporte técnico usuarios, mantenimiento de los equipos
Analista de manufactura	SIM IPC y SCADA	Desarrollo aplicaciones Ingeniería Monitores del SIM Soporte técnico
Programadores (proyectos)	Módulos del ERP	Desarrollo y Soporte Técnico de los Usuarios

Tabla 4.3 Organización del personal interno

En la siguiente Tabla 4.4, se describen los cargos identificados como críticos dentro del área de ingenierías, como son el analista de manufactura, administrador de red que se encargan del correcto funcionamiento de los recursos críticos identificados.

Cargo Crítico	Recursos críticos
Administrador de Base Datos OPERATOR IBM X Series 3650	• IBM Xseries 3650 –Servidor con base de datos Oracle Enterprise Manager 10 g, encargado del Sistema Integrado de Manufactura, posee Windows Server 2003 Release 2 SP2.
Administrador de Red	• DLink DES-3028._Garantizar la conectividad y confiabilidad de la Red de datos de Manufactura para el área de IT como de Ingenierías • Soporte Externo de la empresa TELCONET se tiene enlace dedicado de 2 Mbps con una compartición 1:1
Analista Manufactura Soporte de PC y IPC para el SIM	• IPC Beckhoff C6140-1033._El Computador Industrial destinado para el control de maquinas, se dispone una nueva en bodega y se le restaura con ayuda de Disco Duro Imagen con Acronis True Image, posee sistema Operativo Windows XP SP3 algunos con imagen corporativa. • Simatic Panel PC 677B Es un PC Industrial destinado para el

	control Prensa Vulcanización, posee sistema Operativo Windows XP SP3, y se restaura con disco image. • IBM Lenovo PC Desktop, Computador utilizado para registrar datos al SIM, posee SO Win XP SP3, OPC Server necesario para la interconexión con OPERATOR.

Tabla 4.4 Organización del personal interno

4.5.2 Identificación del impacto y tiempo de interrupción aceptable

En la Tabla 4.5 y 4.6 se especifican los recursos y procesos críticos con los que cuenta el Área de Ingenierías dentro de la empresa Continental Tire Andina S.A, así como el impacto y el tiempo de interrupción aceptable.

Recursos	Impacto	Tiempo
Servidor OPERATOR Aplicación	No se puede acceder al sistema integrado de manufactura, los usuarios no pueden conectarse a la aplicación	8 Horas

Servidor de SCADA Mixer	Los usuarios no pueden acceder a la pantalla de visualización de la maquina	8 Horas
PC IBM lenovo	No se puede registrar el conteo de producción de las líneas de producción, ya sea piezas producidas o metros producidos en el SIM	4 Horas
Equipos de comunicación	Los usuarios no se pueden conectar a la Intranet	1 Día
Cableado estructurado	No existe conexión física entre dispositivos	4 Horas

Tabla 4.5 Recursos, Impacto y tiempo de interrupción aceptable

Procesos/ Aplicaciones	Impacto	Tiempo
HMI Mixer	No se visualiza las ventanas de datos y operación para control de los mezcladores.	4 Horas
HMI Prensa H	No registra valores de procesos de vulcanización y no se puede operar la maquina por falta del Controles e Indicadores	8 Horas

HMI y Control de la maquina Constructora	El usuario no puede arrancar la máquina para fabricar piezas debido a que la aplicación de 8SoftPLC está detenida.	8 Horas
BDD HMI Triplex	Usuario no se puede cambiar el tipo de material a fabricar	1 Hora
Registro Producción	No se registra automáticamente el conteo de piezas o metros producidos dentro del sistema OPERATOR para el SIM. Daño de la conexión con el OPC	1 Horas

Tabla 4.6 Proceso Impacto y Tiempo de interrupción aceptable.

4.5.3 Desarrollo de prioridades de recuperación

Las prioridades de recuperación de los recursos o procesos críticos, se realizan en base a un buen esquema de prioridades de impacto de nivel, como es: Alto, Medio o Bajo. Las prioridades altas se basan en la necesidad de restaurar los procesos y recursos críticos dentro del tiempo aceptable de interrupción; las prioridades medias y bajas reflejan la necesidad de restaurar las capacidades operacionales de forma total sobre un periodo de tiempo más largo. En la Tabla 4.7 se detallan los recursos y las prioridades de recuperación identificadas en el Análisis de Impacto en el Negocio.

Recursos	**Prioridad de Recuperación**
Servidor OPERATOR Aplicación	ALTA

Servidor de SCADA Mixer	ALTA
PC IBM lenovo	MEDIA
Equipos de comunicación	ALTA
Cableado estructurado	MEDIA

Tabla 4.7

Proceso Impacto y Tiempo de interrupción aceptable.

Procesos/ Aplicaciones	**Impacto**
HMI Mixer 1 y 2	ALTA
HMI Prensa H	MEDIA
HMI y Control de la maquina Constructora	MEDIA
BDD HMI Triplex	ALTA
Registro Producción	MEDIA

Tabla 4.8

Proceso Impacto y Tiempo de interrupción aceptable.

4.5.4 Identificación de Controles Preventivos

El área de Ingenierías de la Compañía Ecuatoriana cuenta con algunos controles preventivos que permiten disminuir de alguna manera el riesgo que representan

los diferentes amenazas identificadas en el análisis de riesgo, existen controles tales como:

a) El Centro de Cómputo de IT cuenta ya con moderno sistema de climatización, en una cabina espaciosa y cerrada, para evitar daños en los equipos.
b) Posee sistema de UPS, para la estabilización de los picos de voltaje y shout down al corte de energía.
c) Se utiliza Antivirus corporativo
d) Manejo de Respaldos de las principales aplicaciones y registro de cambios.
e) Respaldo completo (Cold back) de la base de datos de OPERATOR
f) Utilización de Firewall
g) Correcta socialización de las normas y políticas de seguridad y confidencialidad de la información.
h) Existe un correcto procedimiento en caso de incendio establecido por el departamento de Seguridad Industrial de la empresa.

4.6 Etapas de la metodología del BIA

Dentro de las etapas de Análisis de Impacto de Negocia (BIA), que nos ayudarán a identificar los requerimientos de los sistemas, procesos y recursos críticos para luego con esta información determinar las prioridades y definir las posibles estrategias de recuperación tenemos:

Primera Etapa._ Adecuado análisis del Impacto del Negocio como base para un adecuado elaboración del DRP.

Segunda Etapa._ Asignación de prioridades de procesos a recuperar que tienen por objetivo principal definir cuáles son los procesos a ser restablecidos en orden de prioridad.

Tercera Etapa._ Todas las posibles estrategias de recuperación de desastres para restaurar las operaciones y servicios de IT rápida y eficazmente

Cuarta Etapa._ Análisis de resultados

Con esta metodología claramente definida por etapas se ha desarrollado el Análisis de Impacto de Negocio (BIA) dentro de este tema de estudio, siguiendo las mejores prácticas aprendidas a lo largo de la Maestría en Gerencia de los sistemas de Información.

La etapa final del análisis de resultados no hacemos mención dentro de este capítulo ya que dentro de nuestro caso de estudio estará reflejado dentro del capítulo VI, como son las conclusiones y recomendaciones.

Capítulo 5

Elaboración de procedimientos DRP

CAPITULO 5. ELABORACION DE PROCEDIMIENTOS DRP

5.1 Introducción

Para el desarrollo del Plan de Recuperación de Desastres (DRP), la organización debe considerar la estructura en el siguiente esquema:

PLAN DE RECUPERACIÓN DE DESASTRES

FUENTE: Disaster Recovery Planning

AUTOR: Jon William Toigo

Fig. 3 Esquema del Plan de Recuperación de Desastres (DRP)

En el Plan de Recuperación de Desastres para Continental Tire Andina S.A., no se considera la etapa de implementación debido a que este es un prototipo.

5.1.1 Diseño del Prototipo del DRP

El diseño del Prototipo de Plan de Recuperación de Desastres (DPR), permite desarrollar una guía que facilita la recuperación de los equipos y aplicaciones que soportan procesos críticos en el Área IT de Continental Tire Andina S.A., el Prototipo permite mantener la continuidad de las operaciones y minimizar el tiempo de interrupción de los procesos críticos, ocasionados por la pérdida o deterioro en la efectividad de los sistemas de procesamiento automatizados, causados por una eventual destrucción/daño temporal o permanente de las instalaciones o equipos del Área IT debido a la presencia de amenazas naturales, humanas o ambientales.

El diseño del Prototipo del Plan de Recuperación de Desastres (DPR) para Continental Tire Andina S.A, se desarrolló sobre la base de las etapas que se especifican en la figura

ESQUEMA DEL PROTOTIPO DEL PLAN DE RECUPERACIÓN DE DESASTRES

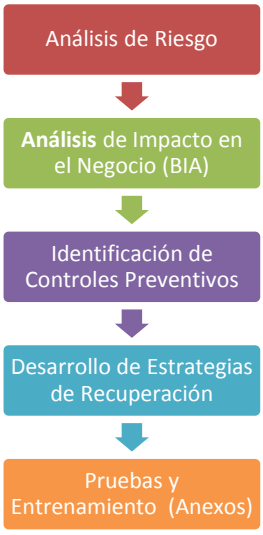


Figura 4. Diseño del Prototipo del Plan de Recuperación de Desastres (DPR)

Cada etapa del diseño del Prototipo se ha estructurado de la siguiente manera:

ANÁLISIS DE RIESGO

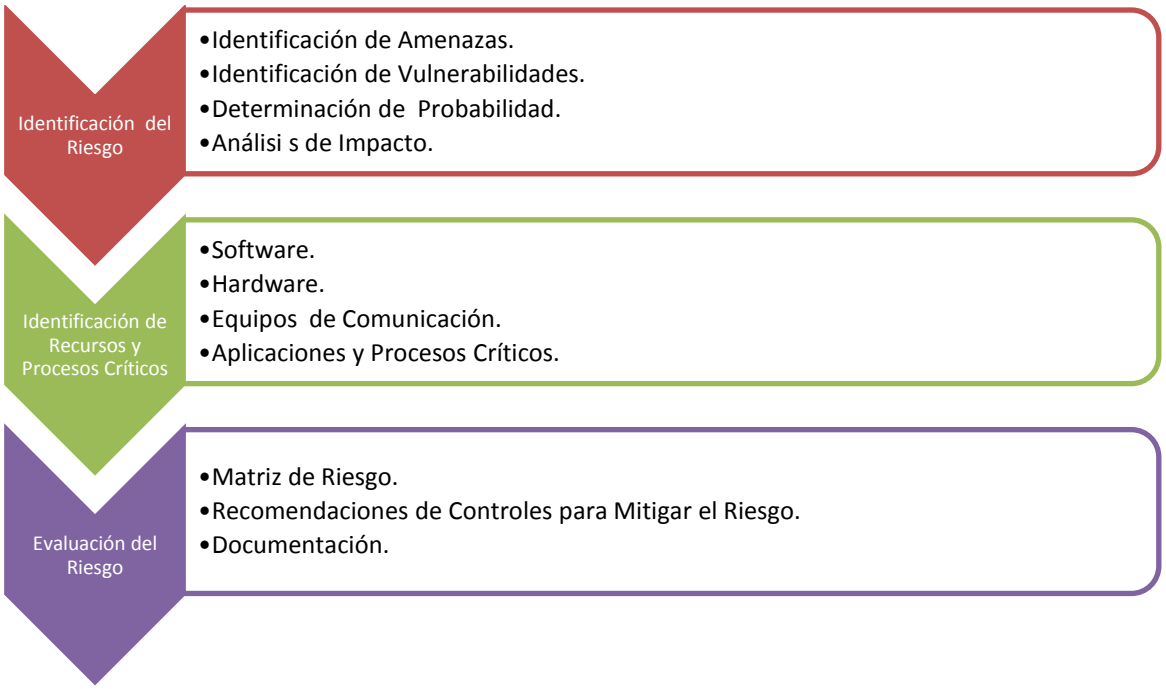


Fig. 5. Esquema del Análisis de Riesgo

ANÁLISIS DE IMPACTO EN EL NEGOCIO E IDENTIFICACIÓN DE CONTROLES

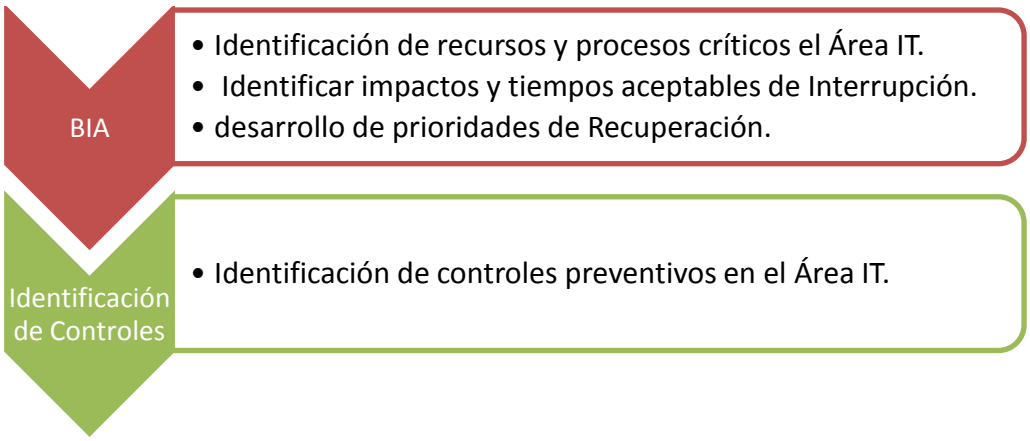


Fig. 6 Esquema del Análisis de Impacto en el Negocio (BIA) e identificación de controles

ESTRATEGIAS DE RECUPERACIÓN DE DESASTRES

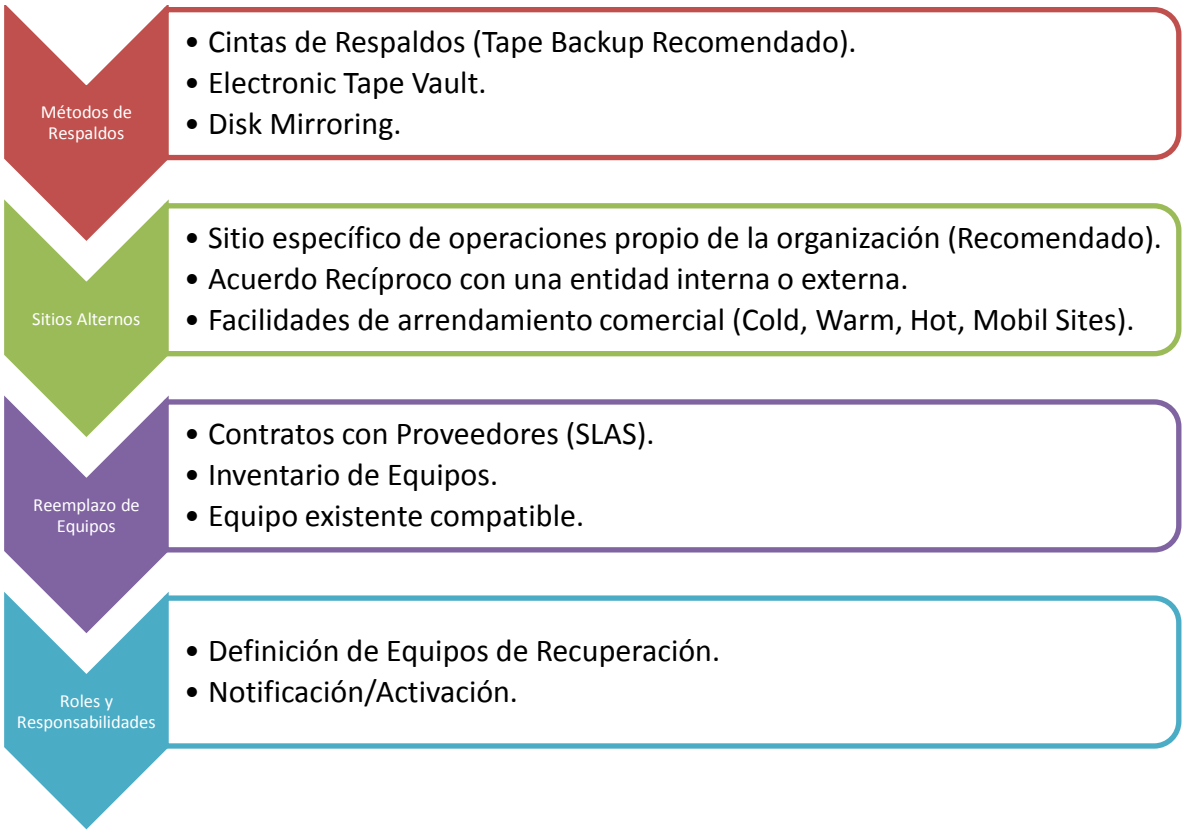


Fig. 7 Esquema del desarrollo de estrategias de recuperación de desastres.

PRUEBAS, ENTRENAMIENTO Y MANTENIMIENTO

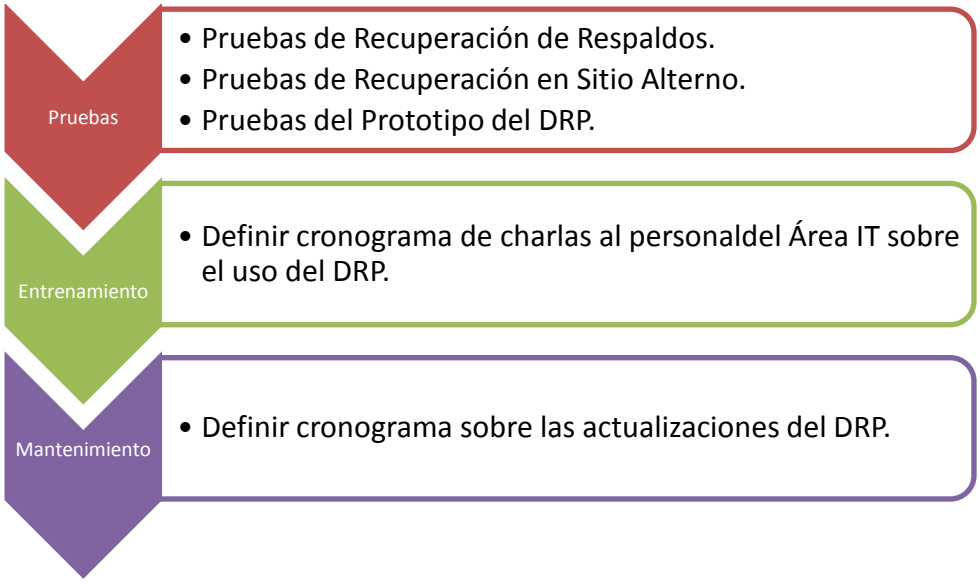


Fig. 8 Esquema de pruebas, entrenamiento y mantenimiento.

5.2 Propósito de estrategia de recuperación

El propósito principal al elaborar el presente trabajo de titulación, es entregar a la empresa el prototipo que facilite la restauración de las aplicaciones de Ingeniería como son SIM, Servidores SCADA, configuraciones de IPC para proceso, etc de forma rápida y que minimice los efectos de pérdidas económicas por daño de maquinas o falta de servico de registro de la producción.

Para definir las estrategias de recuperación que se debe implementar en el Área Ingenierías de Continental Tire Andina S.A., se ha considerado establecer procedimientos para realizar los respaldos (Backups) de las IPC, Computadores estación de la máquina, Software y de la información más relevante que la empresa posee.

Una vez establecidos los procedimientos para realizar los respaldos, se definen los posibles escenarios de desastres y sus respectivas estrategias de recuperación.

5.3 Objetivo

El objetivo de este capítulo es crear una guía para el plan de contingencia en caso de presentarse eventualidades, desastres, en el sistema integrado de manufactura (SIM), dentro del departamento de Ingenierías de la Empresa Continental Tire Andina, basado en estándares y normas fijadas por la división de TI de Continental Tire Américas.

Analizar los sistemas existentes dentro del departamento de Ingenierías para definir requisitos previos, como el tipo de información, aplicaciones (SIM, SCADA, etc.), infraestructura, entre otras.

Especificar técnicamente los requisitos en base a los estándares y normas fijadas por Continental Tire Américas, necesarios para establecer, implantar e implementar un DRP dentro del departamento de Ingeniería de la empresa Continental Tire Andina S.A.

Definir una Metodología basada en el o los estándares fijadas por Continental Tire Américas, que permita elaborar el plan de contingencia y salvaguardar la información de las diferentes Aplicaciones administradas por el Departamento de Ingeniería de la Empresa Continental Tire Andina S.A.

5.4 Responsables

Dentro del desarrollo de las estrategias planteadas para la implementación del DRP, es importante definir previamente los roles y responsabilidades que se le debe asignar al personal y los equipos apropiados para poder desarrollar las tareas.

Dependiendo del tamaño de la organización el personal de recuperación de desastres puede estar asignado a uno o varios equipos específicos que responderán al evento y se encargarán del proceso de recuperación y de devolver el normal funcionamiento del sistema.

Los equipos de trabajo requeridos para la recuperación después de que se ha presentado una interrupción o desastre en el área, se basan en los sistemas y recursos afectados.

El tamaño, los títulos y el diseño de la jerarquía de los equipos dependen de la organización. A continuación exponemos los algunos equipos que pueden formar parte del Plan de Recuperación de Desastres:

- Equipo de Valoración y Monitoreo
- Equipo de Recuperación de Servidores
- Equipo de Recuperación de aplicaciones
- Equipo de Operaciones de la Red
- Equipo de salvamento de Hardware

Generalmente cada equipo tiene un líder que dirige el funcionamiento adecuado del equipo, en nuestro caso esta función estaría a cargo del jefe del área de IT, y para nuestro caso del departamento de Ingenierías, el analista de manufactura es el que cumple el rol fundamental para restaurar, monitorear, salvamento de hardware, control de cambios, de las aplicaciones en ingeniería conjuntamente con el Departamento Electrónico de la planta.

En la planta existe personal de mantenimiento electrónico encargado del monitoreo del sistema SIM (Operator), que liderados del analista de manufactura (personal IT), es el que brinda soporte para recuperar en caso de daños de los equipos o problemas de conexión en la red, laborando en turnos rotativos.

5.5 Desarrollo

5.5.1 Procedimiento para realizar respaldos (Backups) de los servidores de Continental Tire Andina S.A.

A continuación se detallan los procedimientos para realizar los respaldos de la información de los servidores y aplicaciones considerados críticos para Continental Tire Andina S.A.

5.5.1.1 Procedimiento para realizar respaldos del Servidor Principal – SERVER_OPERATOR

- Respaldar diariamente en cintas (Tape) la información del servidor principal donde se encuentran las carpetas de los usuarios de las diferentes Áreas de Continental Tire Andina S.A., definidas de la siguiente manera: Reportes a Producción (Área de Planta Común, Construcción, Vulcanización y Acabado Final). Además se deben respaldar los datos de Inventarios y datos históricos de la producción para los reportes mensuales y trimestrales de producción.
- El método para la obtención de respaldos es Full Backup.
- Cada cinta (Tape) deberá estar etiquetada de la siguiente manera:

Nombre:	**Fecha:**	**Hora:**	**Sitio:**
Data #1	dd/mm/aa	hh:mm:ss	Primario

- Cada tres meses se adquieren 12 cintas para respaldar la información más crítica del negocio, 8 de las cuales se utilizaran en el Sitio Primario, mientras que las 4 cintas restantes se enviaran al Sitio Alterno para salvaguardar la información en caso de desastre.

- Durante las dos primeras semanas de cada mes se utilizaran las 8 cintas para los respaldos diarios, por ejemplo el lunes se deberá etiquetar la cinta como Data #1, y de esa manera se etiquetaran las cintas restantes hasta llegar a la Data #8. El tercer lunes del mes en curso se reutilizara la cinta Data #1 y de esa manera se rotaran las cintas correspondientes al Sitio Primario durante los tres meses.

- Cada viernes se obtendrá una cinta adicional que se le enviara al Sitio Alterno. Esta cinta estará etiquetada de la siguiente manera:

Nombre:	**Fecha:**	**Hora:**	**Sitio:**
Data #4v	dd/mm/aa	hh:mm:ss	Alterno

- Cada *cierto día de la semana* se deberá enviar la cinta del día viernes etiquetada como Sitio Alterno, al Centro Alterno escogido por la organización. Debido a la política de confidencialidad de la planta no podemos mencionar esto en este presente trabajo de dominio público.
- Las cintas etiquetadas como Sitio Primario se almacenaran en la caja fuerte del Área IT de Continental Tire Andina S.A.
- Una vez que las cintas del Sitio Primario, han cumplido el cronograma de rotación durante los tres meses se las envía a la caja fuerte del Sitio Alterno.
- Este procedimiento incluye el respaldo de BDD

5.5.1.2 Procedimientos para realizar respaldos (Backups) del Software y Aplicaciones utilizadas en Continental Tire Andina S.A.

- Es necesario realizar el respaldo de todo el software y sus respectivas licencias, así como de aplicaciones utilizadas por la organización en discos compactos para de esta manera estar preparados ante cualquier situación de interrupción provocada por problemas con el software que afecte el normal desempeño del negocio.

- En el caso de la IPC es necesario crear puntos de restauración dentro del mismo Disco Duro, además de extraer una COPIA Imagen del todo el Duro, con ayuda de los software llamado ACRONIS TRUE IMAGE, utilizado en otras plantas de Continental para respaldar aplicaciones.

- Para los PC utilizados para registro de la producción del SIM, se debe guardar el archivo de respaldo de la Configuración del OPC Server utilizado para enlazar los datos del PLC con el OPERATOR, razón por la cual se debe documentar el nombre de los variables con su respectiva fecha.

- Una copia del software y las aplicaciones se almacenaran en el Sitio Primario, dentro de la compañía, claramente identificadas

- Para el caso de Licencias de los programas utilizados para desarrollo de aplicaciones electrónicos como la programación de PLC, sacar su respectiva copia en disco compacto del programa con su respectiva licencia y registrar en el inventario de software del departamento.

- Cada vez que se adquiere nuevo software, o exista actualizaciones se las aplicaciones se debe obtener una copia de seguridad en discos compactos, las cuales se distribuyen de la siguiente manera: una copia para el Sitio Primario.

- Para el caso de sistemas operativos embebidos se debe realizar una copia física de la Unidad de almacenamiento, puede ser Disco Duro IDE o SATA, Compact Flash, PenDrive, que debe reposar en el Sitio Primario en nuestro caso Oficina del Analista de Manufactura.

5.5.2 Estrategias de Recuperación ante posibles escenarios de desastres.

A continuación se presentan las estrategias de recuperación ante posibles escenarios de desastres, para cada recurso crítico identificado en el BIA y que forma parte del Área IT y del Departamento de Ingenieras de Continental Tire Andina S.A.

Daño de Hardware (Fuente de Poder, Ventiladores, Discos Duros quemados o dañados), que no permita acceder a este equipo.	
Estrategia de Recuperación	**Tiempo de Recuperación**
El Analista de manufactura debe identificar con ayuda del proveedor la lista de repuestos críticos y generar la O/C para tener disponible en Bodega.	1.5 Horas
La configuración actual de la red que posee Continental Tire Andina S.A. permite conectarse remotamente con los PC y las IPC y respaldar rápidamente los archivos del PLC y monitorear con ayuda de Escritorio Remoto	0.5 Hora
Otra estrategia que puede considerarse es instalar	3 Horas

Servidor de Imágenes para respaldar vía Red las Imágenes de los Computadores Industriales que controlan maquinaria.	

Daño de Software (Sistema Operativo, Virus, etc.), que no permite funcionar adecuadamente al servidor.	
Estrategia de Recuperación	**Tiempo de Recuperación**
El administrador de la red debe chequear el servidor y analizar si el daño de software se lo puede solucionar sin la necesidad de reinstalar todo el servidor. Si el daño es leve se puede considerar promover a un servidor Backup Domain Controller (BDC) a Primary Domain Controller (PDC) hasta solucionar el problema del servidor.	0.5 Hora
Si el daño implica reinstalación del servicio este procedimiento tomara más tiempo y de igual forma se debe considerar promover a un servidor Backup Domain Controller (BDC) como Primary Domain Controller (PDC), restablecer los respaldos de Reportes, Costos y la Base de Datos Aduana	3 Horas

Tabla 5.1 Estrategias de recuperación para el Servidor_SIM.

Daño de Hardware (Fuente de Poder, Ventiladores, Discos Duros quemados o dañados), que no permitan acceder a este equipo.	
Estrategia de Recuperación	**Tiempo de Recuperación**
El electrónico de Turno con ayuda del Analista de manufactura debe reemplazar la tarjeta dañada sacando de Bodega el repuesto, por ejemplo la fuente de alimentación.	1 Horas
En el caso de que no exista como reparar el equipo cambiar por un equipo nuevo de bodega y colocar el disco imagen que se encuentran almacenado en el área de backups físicos de área de Ingenierías, específicamente el Laboratorio Electrónico.	2.5 Horas
Daño de Software (Sistema Operativo, Bases de Datos, Virus, etc.), el cual no permite funcionar adecuadamente al servidor.	
Estrategia de Recuperación	**Tiempo de Recuperación**
El Analista de manufactura debe analizar el daño de software y si se lo puede solucionar sin la necesidad de reinstalar el servidor o se puede utilizar el punto de restauración del S:O.	0.5 Horas
Si el daño supera el tiempo establecido de recuperación de 1 hora, se procede a cargar directamente el Servidor de BackUp y conjuntamente con Electrónico de Turno realizar las configuraciones del PLC y de la Red. Tener en cuenta de modificar el valor de conteo para el SIM.	3 Horas

Tabla 5.2 Estrategias de recuperación para el Servidor SCADA del Mixer

Daño de Hardware (Fuente de Poder, Ventiladores, Discos Duros quemados o dañados), que no permitan acceder al equipo.	
Estrategia de Recuperación	**Tiempo de Recuperación**
El Analista de manufactura analiza el daño, se detecta una falla en los dispositivos del PC, se dispone de un set de repuestos como son las fuentes de poder, tarjetas de red, discos duros, etc.	0,5 Horas
Continental Tire Andina S.A. cuenta con un PC de Backup lista en el caso de sufrir una daño a nivel para reemplazarla inmediatamente y no perder reporte de piezas producidas en la línea de manufactura.	1 Horas
Daño de Software (Sistema Operativo, Bases de datos, Virus, etc.), el cual no permite funcionar adecuadamente al servidor	
Estrategia de Recuperación	**Tiempo de Recuperación**
El analista de Manufactura contacta con el Administrador de la Red, debe chequear que exista conexión y los servicios de red presentes. También se contacta con el Administrador Base de Datos, de ser el caso debe chequear el servidor y analizar si el daño de software se lo puede solucionar sin la necesidad de solicitar un equipo de respaldo a la empresa OPERATOR System.	5 Horas

Tabla 5.3 Estrategia de recuperación para PC Registro Producción

Daño de Hardware (Fuente de Poder, Ventiladores, Discos Duros quemados o dañados), que provocan daños en los equipos de comunicaciones	
Estrategia de Recuperación	**Tiempo de Recuperación**
Si se presentan daños en los Switch Administrables, Routers, que provoquen la perdida de comunicación con las secciones de la planta como es Construcción y Bodega de Producto y el enlace de internet. El Administrador de Red debe comunicarse con el técnico de soporte del equipo afectado. Si el daño del equipo es irreparable se contacta con el proveedor para gestionar el reemplazo.	3 Horas
Daño en la configuración de los equipos de comunicación: Firewall, Routers	
Estrategia de Recuperación	**Tiempo de Recuperación**
En caso de detectarse problemas en la configuración de firewall y los routers, el Administrador de Red se encarga de contactarse con los proveedores de los equipos, sea de la empresa Telconet para solucionar el problema de comunicación.	1 Hora
Daño en Switch y Hubs de la red interna de Continental Tire Andina S.A.	
Estrategia de Recuperación	**Tiempo de Recuperación**
Si se presentan daños en la fuente de poder, ventiladores internos de los switch y hubs que conectan la red LAN, se procede de inmediato a colocar el equipo	1 Hora

de respaldo, mientras se adquiere un equipo de similares características.	
Daño de cableado estructurado del Área IT	
Estrategia de Recuperación	**Tiempo de Recuperación**
Si se detecta que un patch cord se encuentra dañado, el Administrador de Red se encarga de cambiarlo o en su defecto adquirir uno nuevo.	1 Hora

Tabla 5.6 Estrategias de recuperación para Redes y Equipos de Comunicación de Continental Tire Andina S.A.

Amenazas Naturales (Fuego, Inundaciones, Terremotos, Erupciones volcánicas, etc.) y Amenazas Humanas (Sabotajes, Hackers, Robo, Vandalismo, Huelgas, etc.)	
Estrategia de Recuperación	**Tiempo de Recuperación**
En caso de que las amenazas que puedan prever de alguna manera se proceden a obtener respaldos de las aplicaciones, archivos de los usuarios, instaladores y licencias, etc. Además proteger los equipos del Área con cobertores o evacuarlos de forma que se minimice el impacto producido por el desastre.	56 Horas
Amenazas Ambientales (Polvo, Químicos, Aire Acondicionado, etc.) **Estrategia de Recuperación:** Estas amenazas producen daños físicos a los equipos ubicados en el Área IT,	

para superar estos percances es necesario seguir las estrategias de recuperación descrita en los escenarios correspondientes a daños físicos de los servidores.

Tabla 5.7 Estrategia de recuperación para el Área Ingenierías

NOTA: Se debe considerar que la información recuperada corresponde al último respaldo, razón por la cual es necesario informarles a los usuarios que deben ingresar los datos referentes a las transacciones realizadas antes de que se produzca alguno de los escenarios descritos anteriormente.

Para la definición de los activadores es necesario establecer un esquema que contemple los grupos de trabajo asignados para la recuperación de los procesos críticos del negocio después de que se ha producido un desastre.

5.5.3 Definición de los equipos de Recuperación

Con la colaboración del Jefe de área de IT se determinó los equipos y el personal que participara en el prototipo de Plan de Recuperación de Desastres, dichos equipos estarán conformados por personal del Área de Sistemas y personal de soporte en Ingenierías con el cargo de *Analista de Manufactura*, debido a las necesidades de la Planta, se tomó la decisión estratégica de agregar al grupo de ingenierías una persona fija de IT, involucrada en el soporte y desarrollo de nuevas aplicaciones y que brindara el soporte adecuado al sistema Integrado de Manufactura.

A continuación se presenta en la Fig. 8, un esquema de los equipos designados para la recuperación de desastres una vez activado el Prototipo del Plan de Recuperación de Desastres.

EQUIPOS DE RECUPERACION DE DESASTRES

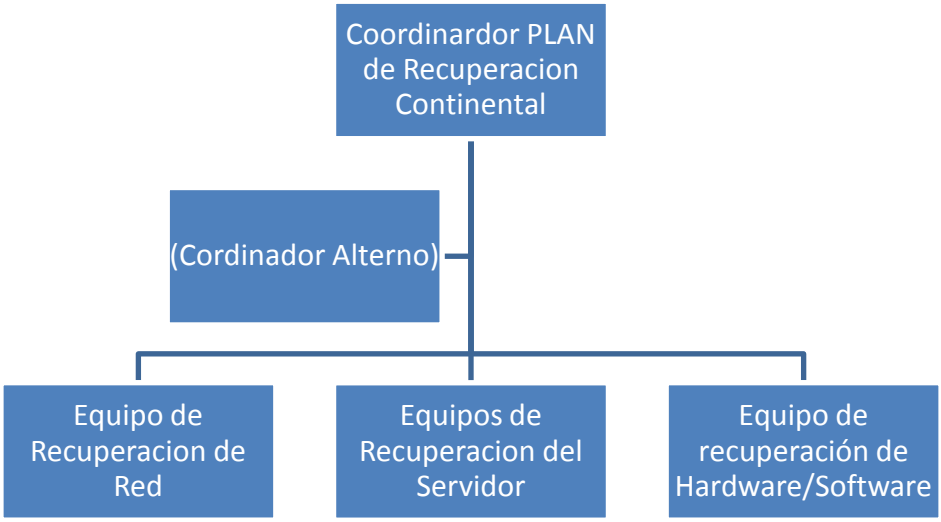


Fig. 8 Esquema de Equipos para la Recuperación de Desastres

Se designó como Coordinador del Plan de Recuperación de Desastres al Jefe del área de IT cuyas responsabilidades se definen a continuación.

- Activar el Prototipo del Plan de Recuperación de Desastres.
- Entrenar al personal que conforma los equipos de recuperación.
- Coordinar con los miembros de los demás equipos.
- Actualizar el Prototipo del Plan de Recuperación de Desastres (DRP).
- Planificar pruebas y simulacros para comprobar el correcto funcionamiento del Plan de Recuperación de Desastres (DRP).

Coordinador Alterno. Se designó al Jefe de Laboratorio Electrónico, como Coordinador Alterno quien tendrá similares responsabilidades en caso de que no se encuentre presente el Coordinador del Plan del Recuperación de Desastres (DRP).

Equipo de Recuperación de Redes Ingenierías Está conformado por personal del Área de Sistemas de Continental Tire Andina S.A. y personal de soporte externo:

- Administrador de Red – Continental Tire Andina S.A.
- Enlaces – Técnico TELCONET
- Configuración de routers – Continental Tire Andina S.A.
- Cableado estructurado. – Proyectel

Este equipo tiene a su cargo las siguientes responsabilidades:

- El Administrador de la Red es el líder del equipo, además se encargara de realizar los contactos con los proveedores de servicios necesarios para restaurar las comunicaciones y redes
- Verificar el correcto funcionamiento del cableado estructurado en el Centro de Computo Alterno.
- Configurar los equipos de comunicaciones (routers, switch, etc.)
- Verificar el funcionamiento de los enlaces

Equipo de Hardware y Software. Este equipo estará conformado por las siguientes personas:

- Administrador de la red – Continental Tire Andina S.A.
- Analista de Manufactura
- Electrónico de Turno

Las responsabilidades del equipo se detallan a continuación:

- El administrador de la red es el líder del equipo, además se encargara de realizarlos contactos con los proveedores de servicios necesarios para

restaurar las configuraciones y el software en los servidores y equipos de Ingenieria.

- Instalación y configuración de los servidores
- Levantar los servicios necesarios (correo electrónico, internet, etc.).
- Recuperación de respaldos.
- Verificar el funcionamiento de los servidores.

Equipo de recuperación de Base de Datos y Aplicaciones SIM. El equipo está conformado por:

- Líder del equipo – Administrador de servidores
- Programador – Continental Tire Andina S.A.

Este equipo tiene a su cargo las siguientes responsabilidades:

- Instalación y configuración de Base de Datos
- Recuperar la información de los respaldos de la Base de Datos.
- Probar el correcto funcionamiento de las Bases de Datos.

NOTA: Los miembros del equipo deben estar familiarizados con las metas y procedimientos de los otros equipos.

5.5.4 Notificación y Activación

Esta fase incluye los métodos para notificar al personal asignado en los equipos establecidos en el prototipo DRP. Entre los métodos de notificación tenemos:

- Contactar al personal a través de teléfonos (casa/celular)
- Correo Electrónico (esta no es una vía segura debido a que la persona puede o no leer el mensaje).

Una vez que se ha evaluado el daño que se ha presentado en el Área IT de Continental Tire Andina S.A., el Coordinador es la persona encargada de activar el Plan. En un inminente desastre, la prioridad es conservar la salud y seguridad del personal antes de proceder a la notificación y activación del Prototipo del Plan de Recuperación de Desastres, que permitirá a la organización recuperar los procesos críticos del negocio. La secuencia de notificación se lista a continuación:

- El primero en ser notificado y responder es el Coordinador, en caso de que no este no se encuentre se procederá a notificar al Coordinador Alterno.
- El Coordinador debe notificar al líder de cada equipo sobre el desastre que se ha presentado.
- El líder de cada equipo se encargara de notificar a los integrantes del equipo.
- Para la notificación se utilizara el listado de personal interno y de soporte externo.

5.5.5 Pruebas de recuperación de Respaldos

Para las pruebas de recuperación de respaldos es necesario realizar las siguientes etapas:

- Definir el personal encargado de realizar las pruebas de recuperación de respaldos.
- Verificar el correcto funcionamiento en la cinta y registrar en la bitácora de respaldos.
- Realizar un cronograma de pruebas de recuperación con la cinta de respaldo de área.
- Probar la integridad de los datos almacenados mediante una prueba de restauración.

- Medir el tiempo de recuperación de los datos almacenados en la cinta de respaldo.

Se sugiere realizar las pruebas de recuperación de respaldos de las cintas que se encuentran almacenados en el área IT y de Ingenierías.

ITEM	CINTA	CAPACIDAD	RESPALDO	FECHA BACKUP	RESPONSABLE	STATUS	RESPONSABLE VERIFICACION
1							
2							
3							
4							
5							

Tabla 5.8 Bitácora de respaldos

Se recomienda el uso de la Tabla 5.8, para realizar el control de las pruebas de recuperación de la información que se encuentran en las cintas de respaldos del área de IT.

5.6 Registros

A continuación tenemos los formatos de los registros utilizados para la verificación de pruebas, que también los podemos encontrar dentro de los diferentes anexos de este presente trabajo:

LISTA DE VERIFICACION PARA PRUEBAS BAKUPS	
Fecha:	Fecha de Recuperación:
Autor:	Código:
Fecha respaldo:	Departamento:
Contenido:	
Servidor donde se obtuvo el respaldo:	
Datos y programas a recuperar:	
Comentarios:	
Revisor por:	
Fecha Revisión:	

Tabla 5.9 Formato para pruebas de Cintas

LISTA DE VERIFICACION PARA PRUEBAS DISCOS IMAGEN IPC	
Fecha:	Fecha de Recuperación:
Autor:	Código Maquina:
Fecha respaldo:	Departamento:
Información del PLC (SoftPLC):	
Computador Industrial donde se obtuvo el respaldo:	
Datos y programas a recuperar:	
Comentarios:	
Revisor por:	
Fecha Revisión:	

Tabla 5.10 Formato para pruebas de Imágenes Computadores Industriales (IPC)

Capítulo 6

Conclusiones y Recomendaciones

CAPITULO 6. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Luego de haber realizado el presente proyecto de titulación, en la cual se entrega una guía que ayudará a la empresa a enfrentar un desastre, provocado u ocasionado por amenazas naturales, humanas, ambientales, permitiéndole minimizar y mitigar los perjuicios económicos alineados con el Plan de Continuidad del Negocio, podemos concluir en los siguientes puntos:

- El análisis de riesgo efectuado en Continental Tire Andina S.A., permitió identificar las amenazas y vulnerabilidades tales como la probabilidad de impacto de riesgo de Inundación debido a la ubicación de la planta a la orilla de un río y riesgo de un desastre aéreo por estar dentro de la ruta despegue y aterrizaje.

- De acuerdo al análisis de riesgo se determino la falla de los computadores (IPC) por efecto de la temperatura, en planta para el control de proceso, debido a la contaminación por Negro de Humo en la planta que especialmente se da en el área de Mescladores.

- Se ha identificado la alta probabilidad e impacto de infección por virus informático por efecto de conectar dispositivos de almacenamiento externos o reproductores de música, etc. en las PC e IPC de registro de datos y control de maquinaria por parte de los obreros.

- Se detectó también la falta de una campaña de socialización de las normas y políticas internas de IT, para el manejo y uso de los recursos informáticos, dirigida a los obreros y empleados de la compañía.

- El Análisis de Impacto en el Negocio (BIA), permitió desarrollar estrategias de recuperación que permiten restaurar los procesos y recursos críticos de la empresa de forma rápida y eficaz.

- Los procedimientos de recuperación establecidos en el DRP, permitirán restaurar en el menor tiempo posible (8 horas = 1 Turno) los procesos críticos del área de Ingenierías (Sistema Integrado de Manufactura, Programas PLC, Configuraciones de OPC, etc.), infraestructura, las comunicaciones de tal forma que la producción de la empresa no se pierde y no genere pérdidas.

- Al realizar las pruebas de recuperación en las IPC se observó que ya se disponen en el mercado Unidades de Almacenamiento IDE, por lo que se migró a otro tipo de unidad de almacenamiento.

6.2 Recomendaciones

Finalmente como resultado del estudio realizado podemos realizar las siguientes recomendaciones:

- Adoptar las presentes guías y planes elaborados en el presente trabajo dentro de la empresa Continental Tire Andina para el Departamento de Ingenierías.

- El jefe del área de IT, siempre debe realizar campañas informativas de las normas y políticas informáticas dentro de la empresa, como es el uso adecuado de los recursos informáticos (internet, suministros, etc.) que deben contar dentro del código de conducta de la compañía.

- Realizar una prueba anual del prototipo del Plan de Recuperación de Desastres (DRP) y actualizarlo permanentemente, de forma que se pueda corregir errores que puedan presentarse.

- Implementar un servidor de Imágenes de las Unidades de Almacenamiento a través de la Red de Ingenierías para facilitar el trabajo en las IPC y no tener que extraer el Disco Duro físicamente.

- Documentar los procedimientos y aplicaciones por motivo de la instalación o adquisición de nueva maquinaria, así como las nuevas aplicaciones desarrolladas por el área de Ingeniería.

- Actualizar periódicamente el Antivirus en las PC remotas donde no se pueda realizar la actualización (Update) de forma automático por medio del servicio de Red.

- Realizar mantenimientos preventivos cada 6 meses de los Computadores utilizados para el registro de la producción dentro de la planta, esto por la contaminación del Negro de Humo. Si es necesario disminuir el periodo de mantenimiento.

- Actualización continúa de las guías y procedimientos conforme a los nuevos equipos y versión de software instalados en los equipos de la empresa o por motivo de adquisición de nueva maquinaria.

- Conforme a la normativa ISO 27000,27001 y 27002 para la Seguridad Informática se aplica conforme a los lineamientos de la empresa los planes desarrollados que deberán ser revisados conforme a nuevas actualización o anexos a la norma vigente.

- Realizar simulacros programados conforme al plan de mitigación propuesto para probar back-ups y entrenamiento del personal.

BIBLIOGRAFIA

Referencias Bibliográficas

Libros, Revistas, Publicaciones:

- **TOIGO, JON WILLIAM,** (2003), Disaster Recovery Planning Preparing for the unthinkable, 3ra Edition, Prentice Hall PTR.

- **INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION**, (2003), Manual de preparación al Examen CISA, Rolling Meadws.

- **PELTIER THOMAS R,**(2001), Information Security Risk Analysis, 1st Edition ADI, Auerbach Pub.

Páginas Web consultadas:

[MEDI01]	Cristian Borghello, Pagina web titulada: Tesis Seguridad Informática – Implicancias e Implementación, 2001 [consultado 04/06/2012], disponible en http://www.segu-info.com.ar
[MEDIO2]	Wikipedia-Enciclopedia Libre, Plan de Recuperación ante Desastres, [consultado 03/03/2012], disponible en http://es.wikipedia.org/wiki/Plan_de_recuperaci%C3%B3n_ante_desastres#mw-head
[MEDIO3]	The Bussiness Continuity Planning& Disaster Recovery Planning Directory, Copyright © 1993-2011 [consultado 15/07/2012], disponible en http://www.disasterrecoveryworld.com/risk.htm